Richmond Journal of Law and Technology

Volume 21 | Issue 3 Article 5

2015

The Big Data Collection Problem of Little Mobile Devices

Michael Arnold

Dennis R. Kiker

THE BIG DATA COLLECTION PROBLEM OF LITTLE MOBILE DEVICES

Michael Arnold* & Dennis R. Kiker**

Cite as: Michael Arnold & Dennis R. Kiker, *The Big Data Collection Problem of Little Mobile Devices*, 21 RICH. J.L. & TECH. 10 (2015), http://jolt.richmond.edu/v21i3/article10.pdf.

[1] There should be little question that mobile device-based data are discoverable if relevant. However, as was the case with ordinary computer-based data a decade or more ago, there is a tendency to believe that there is only one way to collect such data—"forensically."[1] This

* Michael Arnold is a Solutions Program Manager with UnitedLex, a legal process solutions provider. Mr. Arnold has been the Director of Litigation Technology at LeClair Ryan's Discovery Solutions Practice and with UnitedLex as part of their discovery practice in Richmond, Virginia. He has over 22 years in Information Technology and has been providing technical legal solutions for corporate and law-firm clients since 2004. Mr. Arnold has been involved in all aspects of litigation including forensic collections, complex data analysis and presentation and has attended more than 8 cases in various capacities in local state and federal court. Mr. Arnold is now working on developing new technologies and solutions to help clients respond to and address the needs of the next e-Discovery legal challenges.

** Dennis Kiker is consultant at Granite Legal Systems in Houston, Texas. Mr. Kiker has been a partner in an AmLaw 200 law firm, Director of Professional Services at a major e-Discovery company, and a founding shareholder of his own law firm. He has served as national discovery counsel for one of the largest manufacturing companies in the country, and counseled many others on discovery and information governance-related issues. He is an AV rated attorney admitted to practice in Virginia, Arizona and Florida (retired), and holds a J.D., Magna Cum Laude & Order of the Coif from the University of Michigan Law School.

[1] Indeed, there is confusion even about what the term "forensic" means. Some distinguish between a "forensic image" and a "forensic copy" or "forensically sound" collections. A forensic image refers to a "bit-for-bit copy of the data that exists on the original media, without any additions or deletions." Ovie L. Carroll, Stephan K. Brannon

article will demonstrate that there are a number of potentially reasonable ways to collect mobile device data, and that the choice depends, as it does for any other type of information, on the facts and circumstances of the case. We will first examine the proliferation and impact of mobile data. Then, we will survey the case law demonstrating both that mobile data are relevant and that the principle of reasonableness applies to mobile data as it does to any other source. Next, we will outline the various methods for collecting mobile data, any of which might be reasonable under given circumstances. Finally, we will consider other complicating factors that will impact the decision about what type of collection is appropriate under the circumstances of a give case.

I. PREVALENCE AND RELEVANCE OF MOBILE DATA

[2] It goes without saying that mobile devices are ubiquitous. Research by the Pew Research Center shows that:

- 90% of American adults have a cell phone

& Thomas Song, *Computer Forensics: Digital Forensic Analysis Methodology*, U. S. ATTYS' BULL., Jan. 2008, at 1, 2, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab5601.pdf, *archived at* http://perma.cc/D7ZG-E9UJ. In other words, every data element on the source media is collected, including program files, system files, fragmented files, and even blank disk space. *See* R. Lance Fogarty & Gregory Ledenbach, *Deleted Computer Data Uncovered*, THE TEX. INVESTIGATOR, Spring 2009, at 22, 25, *available at* http://www.protegga.com/wp-content/uploads/2014/10/Tali-Article.pdf, *archived at* http://perma.cc/XS8E-78J5. The terms "forensic copy" and "forensically sound" generally refer to a targeted, file-level collection that does not include such things as fragmented data. *See* Thomas Lidbury & Michael Boland, *Technology: Forensically Sound Collection of ESI*, INSIDE COUNSEL (May 11, 2012), http://www.insidecounsel.com/2012/05/11/technology-forensically-sound-collection-of-esi, *archived at* http://perma.cc/65QY-WCAE. In reality, any type of information gathering for litigation purposes is "forensic" according to the definition of the term: "pertaining to, connected with, or used in courts of law or public discussion and debate." *Forensic*, DICTIONARY.COM, http://dictionary.reference.com/browse/forensic?s=t , *archived at* http://perma.cc/63Q8-9TCZ (last visited Mar. 3, 2015).

- 58% of American adults have a smartphone
- 32% of American adults own an e-reader
- 42% of American adults own a tablet computer[2]

[3] These data represent a 37% increase in cell phone ownership since 2000, and a 23% increase in smartphone ownership in less than three years.[3]

[4] The proliferation of mobile devices is not limited to personal use and does not only affect individuals. Indeed, business use of mobile devices is more complex due to the trend towards "bring your own device" ("BYOD") policies, which either allow or require employees to provide their own mobile devices for work use.[4] The obvious result is that employees' mobile devices will contain a larger mix of personal and business data, with the corollary result that companies will have to produce more information from a wider variety of mobile devices.[5] In a survey conducted by Norton Rose Fulbright, 41% of the responding companies had to preserve or collect data from employees' mobile devices in support of litigation or investigations, an increase of more than 10% in

[2] *Mobile Technology Fact Sheet*, PEW RES. CENTER INTERNET PROJECT, http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/, *archived at* http://perma.cc/8QTP-RD7K (last visited Mar. 3, 2015).

[3] *See Device Ownership Over Time*, PEW RES. CENTER INTERNET PROJECT, http://www.pewinternet.org/data-trend/mobile/device-ownership/, *archived at* http://perma.cc/EVM3-Y74K (last visited Mar. 3, 2015).

[4] *See, e.g.*, Press Release, Gartner, Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes (May 1, 2013), *available at* http://www.gartner.com/newsroom/id/2466615, *archived at* http://perma.cc/4Z5N-C8DH.

[5] *See, e.g., Mobile Device Analytics: Getting Smart About Smartphones*, DELOITTE (2013), *available at* http://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-fas-mobile-device-discovery-and-investigations-08162013.pdf, *archived at* http://perma.cc/2GG6-3688.

two years.[6] Indeed, in a recent survey by BDO Consulting, "the largest percentage of in-house counsel (22.5 percent) say managing mobile and social networking data is the number one issue they will face in the near future[.]" [7] Not surprisingly, then, mobile devices are becoming increasingly important sources of potentially relevant information.

[5] There was, perhaps, a time when attorneys could legitimately overlook data on mobile devices in some cases. When Blackberry devices dominated the market, and were generally synched to enterprise servers, there was little reason to believe that potentially relevant data existed on the mobile device that was not available from a more accessible source.[8] That has changed. First, there is a wide variety of information on mobile devices that is likely not available anywhere else. Types of data available on a smartphone or tablet include:

- E-mail
- Text messages
- Voicemail messages
- User information stored as mini-databases or structured text files (e.g., address books, call history, favorite telephone numbers, browser history, bookmarks, recent Internet searches, cookies)
- Photographs
- Video recordings
- Voice recordings

[6] NORTON ROSE FULBRIGHT, LITIGATION TRENDS SURVEY REPORT 35 (2014), *available at* http://www.nortonrosefulbright.com/knowledge/publications/115045/norton-rose-fulbrights-10th-annual-litigation-trends, *archived at* http://perma.cc/CN9L-TB7L.

[7] BDO CONSULTING, INAUGURALINSIDE E-DISCOVERY SURVEY 3 (2014), *available at* https://www.bdo.com/getattachment/af620fbc-e3c4-46b9-a642-e9332eab5692/attachment.aspx, *archived at* https://perma.cc/6U4X-CY7U.

[8] *See, e.g.*, Charlie Hiphop, *Why the NSA Doesn't Want You to Have a Blackberry*, CANTECH LETTER (July 23, 2013), http://www.cantechletter.com/2013/07/why-the-nsa-doesnt-want-you-to-have-a-blackberry0723/, *archived at* http://perma.cc/CZ6Q-V4DJ.

- Notes
- GPS data (which may be attached to other files, such as photographs)
- Maps and navigation history
- Wi-fi and cellular location history[9]

[6] Second, the data on a mobile device may be quite relevant even in routine litigation. Consider just two common scenarios, starting with routine vehicle accidents. The National Highway Traffic Safety Administration (NHTSA) reports that in 2012 alone, 3,328 people were killed and approximately 421,000 people were injured in accidents involving distracted driving.[10] Current research confirms that the risk of accidents increases significantly with the use of mobile devices while driving.[11] Further, an estimated 9% of all drivers do so while using a cell phone or sending and receiving text messages.[12] Driver conduct is an issue in just about every automobile accident case, and mobile devices are increasingly becoming a key source of evidence on that issue.[13]

[9] *See* Michael Arnold, Column, *Collecting Data from Mobile Devices*, 40 LITIG. 53, 54–55 (2013).

[10] Nat'l Highway Traffic Safety Admin., *Distracted Driving: Facts and Statistics*, DISTRACTION.GOV, http://www.distraction.gov/get-the-facts/facts-and-statistics.html, *archived at* http://perma.cc/A8BE-G6X8 (last visited Mar. 3, 2015).

[11] *See, e.g.*, Sheila G. Klauer et al., *Distracted Driving and Risk of Road Crashes Among Novice and Experienced Drivers*, 370 NEW ENG. J. MED. 54, 57 (2014*), available at* http://www.nejm.org/doi/full/10.1056/NEJMsa1204142, *archived at* http://perma.cc/PT4V-24L7 (showing that dialing, reaching for, or using a cell phone to send or receive text messages increased the odds of an accident by as much as eight times).

[12] *See id.* at 55.

[13] *See id.*

[7] On the business side of litigation, mobile devices are no less important. Some estimates indicate that there has been a 43% increase in the use of instant messaging through mobile devices as a way employees conduct business.[14] Unlike e-mail and voicemail, text messages are generally not duplicative of data that can be found on the company's network.[15] Whether the case involves allegations of employment discrimination or product liability, individual employees implicated in the litigation are increasingly likely to have potentially relevant information on mobile devices that can be found nowhere else.

A. Emerging Case Law Involving Mobile Data

[8] A number of recent cases have directly addressed mobile data, typically in the context of spoliation. For example, *Calderon v. Corporacion Puertorrique a de Salud* was a sexual harassment case in which the plaintiff selectively retained messages on his cell phone.[16] Records from the plaintiff's mobile service provider indicated that plaintiff failed to produce more than thirty-eight text messages sent from the account of the alleged harasser.[17] The court held that the plaintiff's "decision not to forward or save the unproduced texts and photos from prpng@hotmail.com constitutes 'conscious abandonment of potentially useful evidence' that indicates that he believed those records would not help his side of the case."[18] The court determined that plaintiff's failure to

[14] *See, e.g.*, *OMG—Is This the End for Texting?*, CNBC (Feb. 21, 2014, 4:10 AM), http://www.cnbc.com/id/101406820#, *archived at* http://perma.cc/W7SB-KE4H.

[15] *See, e.g.*, Tom Kaneshige, *Think Deleted Text Messages Are Gone Forever? Think Again*, CIO (Mar. 11, 2014, 8:00 AM), http://www.cio.com/article/2378005/byod/byod-think-deleted-text-messages-are-gone-forever-think-again.html, *archived at* http://perma.cc/2WRD-3M4E.

[16] *See* Calderon v. Corporacion Puertorriquena De La Salud, 992 F. Supp. 2d 48, 51–52 (D. P.R. 2014).

[17] *See id.* at 52–53.

[18] *Id.* at 52.

preserve the text messages "severely prejudice[d]" the defendants, requiring an adverse inference instruction at trial.[19]

[9] *In re Pradaxa (Dabigatran Etexilate) Products Liability Litigation* concerned a nationwide multi-district litigation (MDL) in which the plaintiffs moved for sanctions for spoliation of, among other things, business-related text messages.[20] After noting that the duty to preserve for each of the two defendants arose in February and April, 2012, respectively, the court went on to severely chastise the defendants for failing to institute a legal hold specifically identifying text messaging until October, 2013, even though the plaintiffs had specifically requested text messages in its initial discovery requests, and the defendants' own documents showed that they "directed their sales force to use texts to communicate with their supervisors, district managers, and others."[21] In fact, despite that "[i]t is certainly common knowledge that texting has become the preferred means of communication," the defendants failed to suspend the auto-deletion of text messages on company issued and programmed cell phones.[22] The court ordered the immediate production of any relevant text messages, reserving the right to impose sanctions if the data were not available.[23]

[19] *Id.* at 53.

[20] *In re* Pradaxa (Dabigatran Etexilate) Prods. Liab. Litig., MDL No. 2385, 3:12-md-02385-DRH-SCW, 2014 U.S. Dist. LEXIS 173674, at *56–58 (S.D. Ill. Dec. 9, 2013).

[21] *Id.* at *56–57.

[22] *See id.* at *62–63, *65.

[23] *Id.* at *68; *see also* Freres v. Xyngular Corp., No. 2:13-cv-400-DAK-PMW, 2014 U.S. Dist. LEXIS 44116 at *14 (D. Utah Mar. 31, 2014) (ordering production of plaintiffs' cell phone for inspection and copying); Bailey v. Scoutware, LLC, No. 12-10281, 2014 U.S. Dist. LEXIS 37197, at *17–18 (E.D. Mich. Mar. 21, 2014) (allowing forensic inspection of cell phone by plaintiffs' expert in an attempt to identify allegedly missing text and voicemail messages); Christou v. Beatport, LLC, No. 10-cv-02912-RBJ-KMT, 2013 U.S. Dist. LEXIS 9034, at *37–39 (D. Colo. Jan. 23, 2013) (issuing sanctions where

[10] Lastly, *EEOC v. Original Honeybaked Ham Co. of Georgia* involved the defendant's motion to compel a wide variety of information from the class representatives in this sexual harassment, hostile environment and retaliation case.[24] Based on information discovered on one class representative's Facebook page, the defendant sought production of social media content, text messages, e-mail and other electronically stored information relevant to the plaintiffs' alleged damages, as well as their credibility and bias.[25] The court first found that the types of information sought were no different than any other discoverable information:

> As a general matter, I view this content logically as though each class member had a file folder titled "Everything About Me," which they have voluntarily shared with others. If there are documents in this folder that contain information that is relevant or may lead to the discovery of admissible evidence relating to this lawsuit, the presumption is that it should be produced. The fact that it exists in cyberspace on an electronic device is a logistical and, perhaps, financial problem, but not a circumstance that removes the information from accessibility by a party opponent in litigation.[26]

defendants took no steps to preserve the text messages on an iPhone that was subsequently lost).

[24] *See* EEOC v. Original Honeybaked Ham Co., No. 11-cv-02560-MSK-MEH, 2012 U.S. Dist. LEXIS 160285, at *2 (D. Colo. Nov. 7, 2012).

[25] *See id.* at *7–8.

[26] *Id.* at *3–4.

After determining that the requested information was, in fact, potentially relevant, the court ordered its production.[27] To protect the individual plaintiffs' privacy interests, the court appointed a special master to retrieve all of the data, including text messages on the plaintiffs' cell phones, and submit information believed to be relevant for in camera inspection.[28]

B. Case Law Regarding Collection Methods

[11] As demonstrated above, data on mobile devices will often be relevant and, therefore, subject to preservation and possibly collection. The legal standards applicable to the method chosen to collect that data, however, are no different than the standards applicable to any other relevant information: "Whether preservation or discovery conduct is acceptable in a case depends on what is reasonable, and that in turn depends on whether what was done—or not done—was proportional to that case and consistent with clearly established applicable standards."[29] The determination of whether discovery conduct was reasonable or not, "depends heavily on the facts and circumstances of each case and cannot be reduced to a generalized checklist of what is acceptable or unacceptable."[30]

---

[27] *See id.* at *7–8.

[28] *See id.*

[29] Rimkus Consulting Grp., Inc. v. Cammarata, 688 F. Supp. 2d 598, 613 (S.D. Tex. Feb. 19, 2010).

[30] *Id.*; *see also* Stanley v. Creative Pipe, Inc., 269 F.R.D. 497, 523 (D. Md. Sept. 9, 2010); THE SEDONA CONFERENCE, THE SEDONA PRINCIPLES: SECOND EDITION BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION 28 (Jonathan M. Redgrave et al. eds., 2007) [hereinafter THE SEDONA PRINCIPLES], *available at* http://www.sos.mt.gov/Records/committees/erim_resources/A%20-%20Sedona%20Principles%20Second%20Edition.pdf, *archived at* http://perma.cc/9HGB-C3YE.

[12] In *Nola Spice Designs, LLC v. Haydel Enterprises*, the court addressed the propriety and necessity of forensic images.[31] In that trademark infringement case, the plaintiff sought an order compelling the defendants to, among other things, "submit their computers to an exhaustive forensic examination . . ."[32] The court rejected the plaintiff's request because it "far exceed[ed] the proportionality limits imposed by Fed. R. Civ. P. 26(b)(2)(C)—expressly made applicable to ESI by Rule 26(b)(2)(B) . . ."[33] The court explained:

> [Plaintiff's] request for an exhaustive forensic examination of [defendants'] computers is within the scope of ESI discovery contemplated by Fed. R. Civ. P. 34(a)(1)(A). At the same time, however, such requests are also subject to the proportionality limitations applicable to all discovery under Rule 26(b)(2)(C), including the prohibition of discovery that is unreasonably cumulative or duplicative or that could be obtained from some more convenient, less burdensome or less expensive source, or the benefit of which is outweighed by its burden or expense, when considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake and the importance of the proposed discovery to those issues. Certainly, the Official Advisory Committee Notes to the 2006 Amendments to Rule 34 relating to electronic discovery of the type sought by Haydel counsel caution:
>
> "As with any other form of discovery, issues of burden and intrusiveness raised by requests to test . . . can be addressed

[31] *See* Nola Spice Designs, LLC v. Haydel Enters., No. 12-2515, 2013 U.S. Dist. LEXIS 108872, at *2–3 (E.D. La. Aug. 2, 2013).

[32] *Id.* at *2–3.

[33] *Id.* at *3.

> under Rules 26(b)(2) and 26(c). Inspection or testing of certain types of electronically stored information or of a responding party's electronic information system may raise issues of confidentiality or privacy. The addition of testing and sampling to Rule 34(a) with regard to . . . electronically stored information is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems."[34]

[13] Indeed, although

> [F]orensic computer examinations of the type sought by [plaintiff] in this motion are 'not uncommon in the course of civil discovery, . . . "[c]ourts have been cautious in requiring the mirror imaging of computers where the request is extremely broad in nature and the connection between the computers and the claims in the lawsuit are unduly vague or unsubstantiated in nature."[35]

Courts have only granted motions to compel forensic examinations where "where the moving party has demonstrated that its opponent has defaulted in its discovery obligations by unwillingness or failure to produce relevant information by more conventional means."[36]

[34] *Id.* at *3–6.

[35] *Id.* at *6 (quoting John B. v. Goetz, 531 F.3d 448, 459-60 (6th Cir. 2008) (internal citations omitted)).

[36] *Nola Spice Designs*, 2013 U.S. Dist. LEXIS 108872, at *7.

[14] The Sixth Circuit Court of Appeals reached a similar conclusion in *John B. v. Goetz*.[37] This class action litigation spanning over 10 years involved implementation of the TennCare program in Tennessee.[38] During the course of the litigation, disputes arose about the scope of the defendants' preservation and production of ESI.[39] Following a series of hearing on motions to compel and reconsider, the district court entered an order allowing "plaintiffs' computer expert to make forensic copies of the hard drives of identified computers, including not only those at the work stations of the state's key custodians, but also any privately owned computers on which the custodians may have performed or received work relating to the TennCare program."[40] The defendants filed a motion for an emergency stay and a petition for mandamus, both of which the appellate court granted, finding that the district court's order constituted an abuse of discretion.[41] The court first acknowledged that a "party may choose on its own to preserve information through forensic imaging, and district courts have, for various reasons, compelled the forensic imaging and production of opposing parties' computers."[42] One the other hand, the court cautioned that:

> Civil litigation should not be approached as if information systems were crime scenes that justify forensic investigation at every opportunity to identify and preserve every detail. . . . [M]aking forensic image backups of computers is only the first step of an expensive, complex,

[37] *See* John B. v. Goetz, 531 F.3d 448, 461 (6th Cir. 2008).

[38] *See id.* at 451–52.

[39] *See id.* at 451.

[40] *Id.* at 451.

[41] *See id.* at 456–59.

[42] *John B.*, 531 F.3d at 459.

> and difficult process of data analysis that can divert litigation into side issues and satellite disputes involving the interpretation of potentially ambiguous forensic evidence.[43]

The court found insufficient evidence in the record to suggest that the defendants intentionally deleted relevant information or were unwilling or unable to preserve and produce such information in the future.[44] For this reason, and because the ordered forensic imaging implicated "significant privacy and confidentiality concerns," the court granted the defendants' petition and overturned the district court's orders.[45]

[15] *Lee v. Stonebridge Life Ins. Co.* involved a request for a forensic image of the plaintiff's personal computer and iPhone.[46] *Lee* was a class action lawsuit alleging that the defendant insurance company sent unauthorized text messages to prospective purchasers of its insurance products.[47] During discovery, the defendants sought production of the named plaintiff's personal computer and iPhone for the purpose of capturing a forensic image of each in an attempt to recover copies of any relevant text messages.[48] The court denied the defendants' motion.[49] As

[43] *Id.* at 460 (quoting THE SEDONA PRINCIPLES, *supra* note 30, at 34, 47.

[44] *See John B.*, 531 F.3d at 460.

[45] *Id.* at 460–61.

[46] *See* Lee v. Stonebridge Life Ins. Co., No. 11-cv-43 RS, 2013 U.S. Dist. LEXIS 106654, at *2 (N.D. Cal. July 30, 2013).

[47] *See* Beth Winegarner, *Stonebridge Settles Spam Text Case with 60K Plaintiffs*, LAW360, http://www.law360.com/articles/524843/stonebridge-settles-spam-text-case-with-60k-plaintiffs, *archived at* http://perma.cc/3862-H4M6 (last visited Mar. 6, 2015).

[48] *See Lee*, 2013 U.S. Dist. LEXIS 106654, at *2.

[49] *See id.* at *7–8.

in *Goetz*, the court first acknowledged that Rule 34 permits parties to seek inspection and testing of "data or data compilations . . . stored in any medium."[50] Nevertheless, the court held that the defendants "failed to demonstrate sufficient good cause to warrant the extreme step of allowing it to conduct a forensic inspection of Plaintiff's iPhone and personal computer."[51] The court noted that a backup of the iPhone at issue was available on the plaintiff's personal computer, that the plaintiff had already agreed to search for and produce any relevant information stored on her personal computer, and emphasized that there was no evidence of wrongdoing by the plaintiff: "absent a showing of misconduct on Plaintiff's part such that serious questions exist as to the reliability and the completeness of Plaintiff's expert's search, [the defendant] is not entitled to a forensic examination of Plaintiff's personal computer."[52]

[16] In contrast, *Olney v. Job.Com* is a good example of a case in which forensic images were critical to the court's decision.[53] *Olney* was a class action alleging that the defendants made unsolicited calls to the named plaintiff's cell phone in violation of the Telephone Consumer Protection Act.[54] The defendants requested access to the cell phone and computer the plaintiff alleged were involved in the communications between the plaintiff and the defendants, and the court ultimately ordered the plaintiff

[50] *Id.* at *2–3 (quoting FED. R. CIV. P. 34(a)(1)(A)).

[51] *Id.* at *4.

[52] *Id.* at *4–5, *7; *see also* Bradfield v. Mid-Continent Cas. Co., No. 5:13-cv-222-Oc-10PRL, 2014 U.S. Dist. LEXIS 128677, at *11–12, *14–15 (M.D. Fla. Sept. 15, 2014) (denying request for forensic inspection of plaintiff's counsel's computer where there was no evidence that the information sought was not available from some other source, the "particular information sought [was] known to actually exist," and there was no evidence that information had been wrongfully withheld).

[53] *See* Olney v. Job.com, No. 1:12-cv-01724-LJO-SKO, 2014 U.S. Dist. LEXIS 152140, at *67 (E.D. Cal. Oct. 24, 2014).

[54] *See id.* at *6–7.

to deliver both to a neutral expert for imaging.[55] In a very detailed opinion, the court reviewed the analyses by competing experts of the plaintiff's personal computer to determine whether the plaintiff had deleted relevant information, either intentionally or negligently.[56] The court ultimately determined that the plaintiff had in fact engaged in conduct that was, at various points in the litigation, negligent, grossly negligent, and willful, justifying an adverse inference instruction and monetary sanctions.[57]

[17] The *Olney* opinion is instructive for a number of reasons. First, it involves a situation that exemplifies the need for forensic imaging and analysis: where there are allegations that specific information has been deleted. Second, it illustrates the complexity and potentially high cost of forensic analysis. Here, the parties agreed on a neutral expert to image and analyze the data from the plaintiffs' computer.[58] Apparently unsatisfied with the results of that analysis, each of the parties then obtained permission to retain their own experts to perform independent analyses.[59] These experts proceeded to generate reports, supplemental reports, rebuttal reports, and supplemental declarations, to the point where the court finally declined to consider the last submissions, as "[r]ebuttal expert reports [would be] potentially endless in this circumstance[.]"[60] Finally, the court notes that the plaintiff "retained experienced class-action counsel with three law firms who should have known his computer could contain potentially relevant information," leaving the plaintiff with little

[55] *See id.* at *7–8.

[56] *See id.* at *9–26.

[57] *See id.* at *30–34, *36–42.

[58] *Olney*, 2014 U.S. Dist. LEXIS 152140, at *8.

[59] *See id.* at *10.

[60] *Id.* at *24–27.

excuse for not preserving data on his computer.[61] This underscores the fact that adequate preservation steps will typically obviate the need for forensic collection and analysis.

[18] Finally, *Ackerman v. PNC Bank* demonstrates that sometimes the simplest collection method is adequate to the needs of the case .[62] In her appeal from the magistrate judge's order denying her motion to compel discovery and for sanctions, the plaintiff alleged that the defendants had "inadequately gathered electronically stored information ('ESI') or unlawfully destroyed ESI," and "violated Fed. R. Civ. P. 34(b)(2)(E) by producing hard copy ESI documents without the underlying metadata."[63] The court disagreed, noting on the latter point that:

> Rule 34(b)(2)(E) does not specifically reference the production of metadata, but refers to a party's obligation to produce documents as they are kept "in the usual course of business" or organized and labeled according to corresponding discovery request categories. If the discovery request does not specify the form for producing ESI, Rule 34 requires a party to produce it in the form "in which it is ordinarily maintained or in a reasonably usable form or forms."[64]

It is readily apparent that the case law does not require a specific collection method or form of production for any type of information, including mobile data. Rather, the collection method should be reasonable

[61] *Id.* at *32.

[62] *See* Ackerman v. PNC Bank, No. 12-CV-42 (SRN/JSM), 2014 U.S. Dist. LEXIS 8301, at *5–7 (D. Minn. Jan. 23, 2014).

[63] *Id.* at *2, *5–6.

[64] *Id.* at *6 (quoting FED. R. CIV. P. 34(b)(2)(E)(i)–(ii)).

and appropriate for the circumstances of the case.

II. DEFENSIBLE MOBILE DATA COLLECTION OPTIONS

[19] Having made the determination that information contained on mobile devices is potentially relevant, attorneys must then determine whether to collect the data, and if so, how. In making these decisions, there are many factors to consider, including the complexity and cost of the collection relative to the issues at stake in the litigation. Here, we will first survey the available collection methods and discuss the circumstances under which each might be appropriate. Later in this article, we will also discuss some of the challenges and complicating factors associated with mobile data collection.

A. No Collection

[20] Sometimes, not collecting mobile data is a perfectly reasonable option. For example, if the only data that are potentially relevant to the matter are e-mails, and the company has implemented an insulating technology to secure communications on the mobile device and ensure that all business-related e-mails are synchronized with the enterprise e-mail server, then collecting from the mobile device would yield only duplicate data.[65]

[21] Occasionally, all that is needed with respect to mobile data are call and text logs, and in most cases this information can be obtained via provider bills or specific detail requests that do not require the device itself.[66] While the content of text messages is not shown on bills or

[65] *See ESI & Data Hosting*, DLSDISCOVERY, http://www.dlsdiscovery.net/esi_data_hosting.html, *archived at* http://perma.cc/D2V2-2ZEH (last visited Feb. 9, 2015).

[66] *See, e.g.*, *Billing and Payments, Understanding the Bill*, VERIZON, http://www.verizonwireless.com/support/view-bill-online-faqs/, *archived at* http://perma.cc/VCQ9-ZCEK (last visited Feb. 9, 2015).

generally available without collection from the device, these types of call and text logs are not easily erased by an owner or user and benefit from having an impartial timestamp for time sensitive events such as might be required in a distracted driving case.[67] Cellular providers can also provide cellular tower triangulation data that can identify the approximate location of a mobile device at a given time.[68]

B. Hard Copy Collection

[22] As odd as it might seem, paper may sometimes be a defensible form of collecting mobile data. Most modern mobile devices are equipped with applications that enable wireless printing from the device.[69] In some cases, where metadata are not of interest or at issue, the parties may be perfectly satisfied with paper copies of e-mails, text messages, or other content on a mobile device.[70] Simply because it is possible to collect ESI from mobile devices does not mean that it is necessary in every case.

C. Mobile Device Collection

[23] There are essentially three methods of collecting data from a mobile device: file level collection, logical collection, and physical

[67] *See id.*

[68] *See Cell Phone Tower Triangulation*, INT'L INVESTIGATORS INCORPORATED, http://www.iiiweb.net/forensic-services/cell-phone-tower-triangulation/, *archived at* http://perma.cc/49AP-TPMP (last visited Feb. 9, 2015).

[69] *See, e.g.*, Christopher Null, *Mobile Printing: A Guide for the BYOD World*, PCWORLD (Sept. 16, 2013, 3:01 AM), http://www.pcworld.com/article/2048634/mobile-printing-a-guide-for-the-byod-world.html, *archived at* http://perma.cc/3V9E-AMYU.

[70] *See* Mark Lenetsky, *eDiscovery: Collection of Text Messages*, ADAPTABLE TECHNOLOGIES LLC, http://adaptable-tech.com/ediscovery-r-link/ediscovery-collection-of-text-messages/, *archived at* http://perma.cc/GW7P-XSEM (last visited Mar. 5, 2015).

collection.[71]

1. File Level Collection

[24] The simplest method of collecting data from a mobile device is to essentially treat it as an external hard drive. File level collections focus on active data that can be readily accessed through the device's operating system, the operating system of a partner device (such as a connected computer), or via third party software.[72] This is similar in nature to collecting the active files on a computer, which are the files that can be identified using the computer's operating system, such as Windows.[73]

[25] Depending on the needs of the case, and particularly on the importance of preserving metadata associated with the target files, an active file collection can be accomplished as simply as connecting the device to a partner computer as a USB storage device (external hard drive), and using the computer's operating system to navigate to the target files and copying them to the computer.[74] It is important to note that this method has the highest risk of altering both metadata of the files and the state of the mobile device should a physical image potentially be required

[71] *See* CINDY MURPHY, CELLULAR PHONE EVIDENCE: DATA EXTRACTION AND DOCUMENTATION, *available at* https://mobileforensics.files.wordpress.com/2010/07/cell-phone-evidence-extraction-process-development-1-1-8.pdf, *archived at* https://perma.cc/NWN6-A6JX.

[72] *See id.*

[73] *See* Paul Henry, *Quick Look—Cellebrite UFED Using Extract Phone Data & File System Dump*, SANS DIGITAL FORENSICS & INCIDENT RESPONSE (Sept. 22, 2010, 6:16 PM), http://digital-forensics.sans.org/blog/2010/09/22/digital-forensics-quick-cellebrite-ufed-extract-phone-data-file-system-dump/, *archived at* http://perma.cc/CB63-6XNC.

[74] *See* TIM PROFFITT, FORENSIC ANALYSIS ON IOS DEVICES 3–4, 6–9 (2012), *available at* http://www.sans.org/reading-room/whitepapers/forensics/forensic-analysis-ios-devices-34092/ forensic-analysis-ios-devices-34092 (1).pdf, *archived at* http://perma.cc/4PL3-9T5E.

in the future.[75] On the other hand, steps can be taken to mitigate any alteration of the files on the device or to the metadata of the files collected.[76] Usually a USB write-blocker can be used to preserve the device, but not all devices will communicate with the collections computer with such a device installed.[77]

[26] Where metadata may be at issue or will be important for other reasons (such as culling and filtering), commercial software such as Access Data's FTK Imager, Pinpoint Labs Safecopy or Wide Angle's TouchCopy can be used to ensure that the metadata on both the mobile device and the collection drive are not altered as part of the collection.[78] Manual file copy collections are the most limited in what they can collect, as most devices that are not rooted or jail-broken[79] will limit the accessible areas on the device to maintain application security.[80]

[27] Situations where file level collection might be appropriate include

[75] *See id.* at 10–11.

[76] *See Write Blockers*, FORENSICS WIKI, http://www.forensicswiki.org/wiki/Write_Blockers, *archived at* http://perma.cc/6VXA-9C5L (last visited Mar. 6, 2015).

[77] *See id.*

[78] *See, e.g.*, *Data Acquisition & Preservation*, ACCESS DATA, http://accessdata.com/services/digital-forensics/data-aquisition-preservation, *archived at* http://perma.cc/3EPB-JZHA (last visited Mar. 6, 2015); *SAFECOPY*, PINPOINT LABS, http://pinpointlabs.com/sc2.html, *archived at* http://perma.cc/38QX-NDNY (last visited Mar. 6, 2015); *TOUCHCOPY*, WIDE ANGLE SOFTWARE, http://www.wideanglesoftware.com/touchcopy/index.php, *archived at* http://perma.cc/7JBL-GRNJ (last visited Mar. 6, 2015).

[79] *See, e.g.*, Mary McMahon, *What Is a Jailbroken Phone?*, WISEGEEK, http://www.wisegeek.com/what-is-a-jailbroken-phone.htm, *archived at* http://perma.cc/6ZHX-LR6B (last modified Feb. 15, 2015).

[80] *See id.*

cases where there are no relevant call/messaging logs, and a user has identified a few select files on their mobile device that may need to be collected.[81] File level collection is far superior to having the user e-mail the file to a person collecting the data, such as an IT person, counsel or in-house legal representative, because the latter method creates yet another copy of the file that should be preserved or collected.[82] Some devices can be plugged directly into a prepared collection system and accessed just like a portable hard drive and the files exposed for collection.[83]

2. Forensic Logical Copy

[28] A forensic logical copy involves connecting the mobile device to tools or equipment and copying either everything or selected files from the device or any installed memory devices.[84] During a logical collection, certain data such as pictures, music, e-mail, text messages and other files are copied with tools like FTK imager, Cellebrite and others to other media to be processed, evaluated and reviewed.[85] A logical collection does not copy or access anything that is not on the device and does not copy latent information such as slack-space from deleted files or certain protected areas of a phone unless that device has been modified (often referred to as hacked, rooted or jail broken).[86] Logical images do not

[81] *See, e.g.*, MURPHY, *supra* note 71.

[82] *See, e.g.*, Henry, *supra* note 73.

[83] *See* PROFFITT, *supra* note 74, at 9.

[84] *See id.*

[85] *See* David Ashfield, *Mobile Device Forensics: Data Acquisition Types*, CCL GROUP (May 19, 2014), http://www.cclgroupltd.com/mobile-device-forensics-data-acquisition-types/, *archived at* http://perma.cc/C5RQ-FLW7.

[86] *See id.*

collect unsaved data from volatile memory (e.g. from RAM).[87]

3. Logical Collection of Synchronized Data

[29] When a mobile device is synchronized with another location, it may be reasonable to collect from that location as opposed to the device itself. It will almost certainly be simpler and more cost effective.[88] For example, when a mobile device management system (MDM) is implemented within a company, certain applications are installed, or devices are routinely connected to other systems, the devices may be configured to back up their data to one of several locations[89], including:

- The cloud,
- A dedicated server, application host or file share, or
- A specific partner computer or device.[90]

[30] Care must be taken to ensure that the synchronized location does

[87] *See What Are Our Best Options for Collecting and Synchronizing GIS Field Data?*, WEBMAPSOLUTIONS, http://www.webmapsolutions.com/what-are-our-best-options-for-collecting-and-synchronizing-gis-field-data, *archived at* http://perma.cc/C8AK-QVW4 (last visited Feb. 18, 2015).

[88] *See* Vangie Beal, *What Is Mobile Device Management (MDM)?*, WEBOPEDIA, http://www.webopedia.com/TERM/M/mobile_device_management.html, *archived at* http://perma.cc/7FVM-2TZ7 (last visited Mar. 6, 2015).

[89] *See* Carla Schroder, *6 Data Backup Devices for Small Businesses*, SMALL BUSINESS COMPUTING.COM (Aug. 4, 2014), http://www.smallbusinesscomputing.com/biztools/6-data-backup-devices-for-small-businesses.html, *archived at* http://perma.cc/6EVR-GHSF; *see also The Difference Between Cloud Hosting and Dedicated Servers and What's Right for You*, STEADFAST, http://www.steadfast.net/blog/index.php/cloud/he-difference-between-cloud-hosting, *archived at* http://perma.cc/U82P-TVZ7 (last visited Mar. 6, 2015).

[90] *See, e.g.*, Rene Millman, *Smartphones & Tablets Remotely Wiped in UK Police Custody*, ITPro (Oct. 10, 2014), http://www.itpro.co.uk/security/23273/smartphones-tablets-remotely-wiped-in-uk-police-custody, *archived at* http://perma.cc/EH3U-5DCB.

not materially change between the identification and the actual collection of that source.[91] One of the safest ways to ensure that a synchronized location does not change is to disable the synchronization feature of the mobile device by turning the device off, setting the device to airplane mode and/or not connecting the device to any partner computers, sometimes referred to as "docking."[92] Synchronized locations may also be affected or accessed by more than one device. For instance, Gmail, Dropbox and Facebook are common examples of locations that may be connected to more than one device or be changed from a remote computer even after the intended device has been secured.[93] Further, all data on a mobile device may not be in one central location requiring logical collections from multiple sources.

[31] Importantly, if the synchronized data is in the form of a backup, the type, currency, and format of the data may vary significantly from what is on the mobile device and may require not only a forensic expert to review and analyze, but special software to decode the data.[94] For

[91] *See, e.g.*, *Supreme Court Watch: Ten Key Issues from the Riley Opinion Protecting Cell Phone Data Seized During an Arrest*, FED. EVIDENCE REV. (June 30, 2014), http://federalevidence.com/blog/2014/june/supreme-court-watch-cell-phone-content-protected-under-fourth-amendment, *archived at* http://perma.cc/DR9P-NZ8P.

[92] *See, e.g.*, *Computer Tips and Tricks, Gadgets, How-To, Life-2.0 Style*, TECH BUZZ (Mar. 21, 2009), http://www.techbuzz.in/can-two-people-be-logged-into-the-same-facebook-account-at-the-same-time.php, *archived at* http://perma.cc/ZDJ7-77C2; *see also Remote Wipe Overview*, DROPBOX, https://www.dropbox.com/en/help/4227, *archived at* https://perma.cc/743T-JMJJ (last visited Mar. 6, 2015).

[93] *See, e.g.*, *Create and Delete iPhone, iPad, and iPod Touch Backups in iTunes*, APPLE, https://support.apple.com/en-us/HT204269, *archived at* https://perma.cc/RT4L-HXU4 (last visited Mar. 6. 2015).

[94] *See iCloud Security and Privacy Overview*, APPLE, https://support.apple.com/en-us/HT202303, *archived at* https://perma.cc/FL7M-NQTV (last visited Jan. 27, 2015). Microsoft offers a similar service. *See Back up My Stuff*, WINDOWS PHONE, http://www.windowsphone.com/en-us/how-to/wp8/settings-and-personalization/back-up-my-stuff, *archived at* http://perma.cc/3P9H-RXNM (last visited Mar. 6, 2015). Android users can download apps, such as inDefend, to back up their personal information. *See*

example, a user that regularly receives company e-mail on their mobile device, but only periodically backs that device up to a computer or cloud, would have current e-mail easily collected from the device itself, but only out-of-date backups of files in special formats that would require a forensic analyst to translate.[95]

a. Cloud-Based

[32] The cloud could be one of the locations supplied by vendors of the device such as Apple's iCloud,[96] Google's Drive, Microsoft's SkyDrive; or the cloud could be a subscription service such as DropBox, LiveDrive, BlackBlaze Mozy, Amazon, etc. These services are completely hosted by third-party companies each of which have processes that must be followed if anyone other than the user or the paired device wants to collect the hosted backups.[97]

---

inDefend Mobile Backup, GOOGLE, https://play.google.com/store/apps/details?id=com.dataresolve.android.security.backup&hl=en, *archived at* https://perma.cc/GSQ7-SXNL (last visited Jan. 27, 2015). Except using the Link function on a corporate Blackberry server, Blackberry does not backup e-mail, contacts or calendars. *See User Guide: BlackBerry Link for Windows 1.0, Back Up Your Device Data*, BLACKBERRY, http://docs.blackberry.com/en/smartphone_users/deliverables/49304/lym1340633934452.jsp, *archived at* http://perma.cc/X4XE-ZGPF (last visited Mar. 6, 2015).

[95] *See* Satish B., *iPhone Forensics—Analysis of iOS 5 Backups: Part 1*, INFOSEC INST. (May 3, 2012), http://resources.infosecinstitute.com/ios-5-backups-part-1/, *archived at* http://perma.cc/7N6N-9LQL.

[96] *See* Thomas J. Trappler, *When There's a Third Party in the Cloud*, COMPUTERWORLD (July 30, 2012, 10:42 AM), http://www.computerworld.com/article/2505135/cloud-computing/when-there-s-a-third-party-in-the-cloud.html, *archived at* http://perma.cc/45KH-HD4D.

[97] *See, e.g.*, *Back Up My Stuff*, *supra* note 94; BlackBerry *Business Cloud Services*, BLACKBERRY, http://us.blackberry.com/enterprise/products/cloud-services/overview.html, *archived at* http://perma.cc/DEP4-EJ6Z (last visited Mar. 6, 2015); *see also iCloud: iCloud Storage and Backup Overview*, APPLE,

[33] Each of the major vendors, Apple, Google, RIM and Microsoft, have made provisions for complete or selective backups to be made to their cloud services through cellular or wireless network connections.[98]

[34] As home consumer demand for large storage drives increased, and speeds for residential Internet went up, personal clouds solutions developed, which are generally supplied by hard drive manufacturers as a feature of a home network attached storage (NAS) drive.[99] These solutions from Western Digital, LaCie, Seagate and others allow a central backup to be almost anywhere an Internet connection exists, and may create challenges for coordinating collections.

b. Dedicated Server, Application Host, or File Share

[35] A dedicated server or share is similar to the personal cloud listed above, but with the key distinction of it being a company owned and managed server or share and likely only used for select applications such as Exchange, Evernote, a CRM or sales application or for centralized management of company owned devices.[100] To further demonstrate the complexities in discussing this issue with prospective clients, a company may host their servers in the cloud (e.g., Rackspace or Amazon virtual servers), or may be using Cloud based private applications such as

https://support.apple.com/kb/PH12519?viewlocale=en_US&locale=en_US (last visited Mar. 6, 2015), *archived at* https://perma.cc/BFB4-VBDA.

[98] *See, e.g.*, sources cited *supra* note 97.

[99] *See, e.g.*, Margaret Rouse, *What Is Network-Attached Storage (NAS)?*, SEARCH STORAGE (Aug. 2014), http://searchstorage.techtarget.com/definition/network-attached-storage, *archived at* http://perma.cc/RN4Q-32YJ.

[100] *See, e.g.*, Margaret Rouse, *Dedicated Server Definition*, TECHTARGET (Sept. 2005), http://searchsoa.techtarget.com/definition/dedicated-server, *archived at http://perma.cc/BSX6-XR6D*.

Office365 or Exchange Online.[101] Unless an MDM is being used by a company to perform complete backups of mobile devices to one of these central servers, only select data would be available from these locations and typically would not include device only data such as call logs, text messages, local pictures or downloaded files.[102]

i. Partner Computer or Device

[36] A partner computer might be used to synchronize select information to a mobile device or even as a complete backup in the event of loss of the mobile device. iTunes on a local PC or Mac is an example of a computer application that creates a partnership with an iPhone and allows a complete backup of the device to be stored on the computer.[103] An iTunes backup is the closest alternative to an actual logical collection from a physical iPhone.[104] Although the information in iPhone backups is either encrypted or obfuscated in proprietary file formats and naming conventions,[105] others companies like Microsoft or Google, store the

[101] *See, e.g.*, Barney Beal, *Public vs. Private Cloud Applications: Two Critical Differences*, TECHTARGET (May 2012), http://searchcloudapplications.techtarget.com/feature/Public-vs-private-cloud-applications-Two-critical-differences, *archived at* http://perma.cc/D6WB-S68S.

[102] *See Why Mobile Device Management*, 2X, http://www.2x.com/mdm/why-mobile-device-management/, *archived at* http://perma.cc/4824-7JSE (last visited Mar. 6, 2015).

[103] Satish B., *Forensic Analysis of iPhone Backups*, EXPLOIT DB, http://www.exploit-db.com/wp-content/themes/exploit/docs/19767.pdf, *archived at* http://perma.cc/39FT-EPLV (last visited Mar. 16, 2015).

[104] *See* Bader & Baggili, *iPhone 3GS Forensics: Logical Analysis Using Apple iTunes Backup Utility*, 4 SMALL SCALE DIGITAL DEVICE FORENSICS J. 1 (2010), *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.185.4439&rep=rep1&type=pdf, *archived at* http://perma.cc/N4AS-J6DV.

[105] *See, e.g.*, Selena Ley, *Processing iPhone / iPod Touch Backup Files on a Computer*, THE APPLE EXAMINER, http://www.appleexaminer.com/iPhoneiPad/iPhoneBackup/iPhoneBackup.html, *archived at* http://perma.cc/X7VK-HBRH (last visited Mar. 5, 2015).

backups of files in their original format and have industry standard .XML file formats for data such as call logs and text messages.[106]

[37] Some devices can become partners of other mobile devices through peer-to-peer network and wireless connections such as Bluetooth[107] and Near Field Communications (NFC).[108] Peer devices can be either other smartphones, tablets or computers which might have data such as contacts, pictures or files, or they may be more passive devices with limited usage information.[109]

[38] Regarding each of these locations above, it is important to note that only backed up data can be collected from synchronized device locations, and that volatile data (RAM) and information changed on the device since last synchronization will not be available.[110] Further, some companies,

[106] *See , e.g.*, *FAQ about SMS Backup & Restore*, ANDROIDSTUFF (Apr. 18, 2012), http://android.riteshsahu.com/misc/faqs-about-sms-backup-restore, *archived at* http://perma.cc/UMR9-U477.

[107] *See, e.g.*, *Fast Facts*, BLUETOOTH SIG, INC., http://www.bluetooth.com/Pages/Fast-Facts.aspx, *archived at* http://perma.cc/B5JN-ANJE (last visited Mar. 3, 2015).

[108] *See, e.g.*, NEAR FIELD COMMUNICATION, http://www.nearfieldcommunication.org, *archived at* http://perma.cc/EXM3-GT56 (last visited Mar. 3, 2015).

[109] Peer devices go beyond just passive ear pieces and are a growing market with the increase in 'wearable' technologies such as smart watches, fitness bands, health meters and even pain management devices and can be important in litigation due to their ability to either allow files to move from the device without traditional e-mail or text transmissions or for the data that they might supply. *See* Sean Greene, *Electronic Evidence Expert Witness: Will Fitbit and Crowdsourcing* Change Personal Injury Cases?*, EVIDENCE SOLUTIONS, INC., http://www.evidencesolutions.com/web/Digital-Evidence-Articles/fitbit-data-goes-to-court-electronic-evidence-expert.html, *archived at* http://perma.cc/Z58Z-GQET (last visited Mar. 3, 2015).

[110] *See* RICK AYERS ET AL., NAT'L INST. OF STDS. & TECH., U.S. DEPT. OF COMMERCE, GUIDELINES ON MOBILE DEVICE FORENSIC 3, 6 (Special Pub. 800-101, Rev. 1, May 2014), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf, *archived at* http://perma.cc/U7SV-DWU9.

such as Apple, use special formats and mini-databases for the files stored as backups,[111] while others such as Microsoft or Google store the backups of files in their original format and have industry standard .XML file formats for data such as call logs and text messages.[112]

3. Physical Imaging/Full Forensic Copy

[39] A forensic image is a bit-level copy of all data on a device in manner that represents the entire state of the device and could clone an exact duplicate with equivalent hardware.[113] Physical imaging, performed while the device has maintained constant power-on and has been isolated from radio communications, can collect volatile memory, current state of running programs etc.[114] Physical imaging is limited, as logical collection, to data that are on or in the physical device and memory cards.[115] It should be highlighted that UICC (SIM) cards are a type of memory card like removable memory cards (SD & Micro SD) and need to be included in the collection plan.[116]

---

[111] *See, e.g.*, Selena Ley, *Processing iPhone / iPod Touch Backup Files on a Computer*, THE APPLE EXAMINER, http://www.appleexaminer.com/iPhoneiPad/iPhoneBackup/iPhoneBackup.html, *archived at* http://perma.cc/K3KW-K3RH (last visited Mar. 5, 2015).

[112] *See, e.g.*, *FAQ about SMS Backup & Restore*, ANDROIDSTUFF (Apr. 18, 2012), http://android.riteshsahu.com/misc/faqs-about-sms-backup-restore, *archived at* http://perma.cc/TM2Y-YH8W.

[113] *What is Forensic Hard Drive Imaging*, FORENSICON COMPUTER FORENSIC SPECIALISTS , http://www.forensicon.com/resources/articles/what-is-forensic-hard-drive-imaging/, *archived at* http://perma.cc/3NUC-XM9T (last visited Mar. 3, 2015).

[114] Kristine Amari, *Techniques and Tools for Recovering and Analyzing Data from Volatile Memory*, SANS Institute InfoSec Reading Room (Mar. 26, 2009), *available at* www.sans.org/reading-room/whitepapers/forensics/techniques-tools-recovering-analyzing-data-volatile-memory-33049, *archived at* http://perma.cc/5B8D-8EDK.

[115] *See* RICK AYERS ET AL., *supra* note 110, at 46.

[116] *Id.* at 7.

[40] The following table will highlight some of the differences in data that is available from each type of collection listed above.[117]

Table 1.

	Synchronized location	**Logical Device**	**Physical Image**
E-mail Messages	Yes	If stored on phone	If stored on phone or in slack space
Text Messages	No	Yes	Yes
Photos on Phone	No, unless synced	Yes	Yes
Photos uploaded to Web	Yes	No	If in slack or temp space
Voice, video and other Files on Phone	No, unless synced	Yes	Yes
Files uploaded to Web or Server	Yes	No	If in slack or temp space
Internet & Search History	Depends if logged in.	Yes	Yes
Contacts	No, unless synced	Yes	Yes
GPS information	No, unless using GPS App like Garmin or MapMyRun	If GPS enabled and used	If GPS enabled and used
Maps and navigation history	No	May be limited	Yes

[117] *See supra* notes 113–16 and accompanying text.

Wi-Fi Information	No	Networks used, signal etc.	Networks used, signal etc.
Cell Tower information	No	May be limited	Yes
Call history	See provider website	Yes	Yes
Application information	Depends on app and settings	May be limited	Yes

[41] There are multiple ways to collect from mobile devices in a forensically sound manner, and there may be a need for more than one way even in a single case. Forensic collection does not mean only imaging, and imaging does not mean collecting everything.[118] Even the seemingly simple options that one would consider for traditional computers or servers quickly become very complex problems when we approach mobile systems.

III. COLLECTION AS PART OF A LARGER PROCESS

[42] What we call 'collecting' from a mobile device is actually 'processing'[119] and involves a series of steps that are part of an overall process of forensic handling[120] that can be challenged if not handled properly. There are many considerations in certain litigation such as authentication of the actual device (who was the actual user at a point in time), and whether the device is being collected pursuant to a warrant,

[118] Matthew Nelson, *The Top 3 Forensic Data Collection Myths in eDiscovery*, SYMANTEC EDISCOVERY BLOG (Aug. 7, 2013), http://www.symantec.com/connect/blogs/top-3-forensic-data-collection-myths-ediscovery, *archived at* http://perma.cc/ZL5C-EC7L.

[119] *See, e.g.*, Murphy, *supra* note 71.

[120] *See* AYERS ET AL., *supra* note 110, at 2–3.

arrest or consent that go beyond the scope of this writing.

[43] Before we can collect anything, we must identify not only what systems we need to collect from, but how those systems may interact with other systems and make preparations to secure and preserve the data.[121] By being constantly connected, mobile devices are constantly gathering data to internal and external locations. A mobile device can store potentially relevant information on removable memory cards, SIM cards, and internal volatile and non-volatile memory.[122] When certain mobile devices such as the Blackberry go into a 'locked' state, volatile memory is wiped by the device automatically.[123] Additionally, certain methods of unlocking a locked mobile device may require a restart of that device causing certain information to be changed or volatile memory to be cleared.[124] If a device is not protected, incoming calls, text messages, e-mails or application notifications could still change the state of the device even without any malicious intent.[125]

---

[121] *See* MURUGIAH SOUPPAYA & KAREN SCARFONE, NIST SPECIAL PUBLICATION 800-124 REVISION 1: GUIDELINES FOR MANAGING THE SECURITY OF MOBILE DEVICES IN THE ENTERPRISE 5–6 (2013), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf, *archived at* http://perma.cc/FF9G-B38U.

[122] *See* AYERS ET AL., *supra* 110, at 6–8, 10–11.

[123] *Any Way to Prevent Device Wipe after Failed password Attempts in BB10?*, CRACKBERRY (May 22, 2013), http://forums.crackberry.com/blackberry-z10-f254/any-way-prevent-device-wipe-after-failed-password-attempts-bb10-810021/, *archived at* http://perma.cc/Z9TV-L3U4.

[124] *Ensure Mobile Device Security*, 2X MDM, http://www.2x.com/mdm/mobile-device-security/, *archived at* http://perma.cc/V489-LJ2W (last visited Mar. 3, 2015).

[125] Jason Gonzalez & James Hung, Stroz Friedberg LLC, *Mobile Device Forensics: A Brave New World?*, BLOOMBERG LAW REPORTS, http://www.strozfriedberg.com/files/Publication/224ca0f8-5101-4e1b-938a-4d4b128ad5ed/Presentation/PublicationAttachment/ef4a28ad-ff7d-4014-aea8-80505789b86c/Mobile%20Device%20Forensics_%20A%20Brave%20New%20World.pdf, *archived at* http://perma.cc/ZR43-D9RF (last visited Mar. 3, 2015).

[44] Several very significant issues must be considered when approaching the collection of mobile devices:

- Ownership of the device,
- Expected cooperation of the owner and/or user (which may not be the same person or entity),
- Synchronized peer devices,
- Remote access/management and control to the device,
- Technologies and versions, and
- Nature of litigation.[126]

[45] Ownership of the device can complicate matters due to the potential for restricted access such as pin codes, encryption, locks, and overall permission.[127] In many instances where a company maintains ownership of the device or has established clear policies regarding cooperation by employees with shared use devices this may not be an issue, and even passwords, passcodes, pin codes, or encryption keys may be easily obtained.[128]

[46] As individuals become more aware of and sensitive to the amount of data that their mobile devices contain, they are employing more methods of securing the data and devices through PIN codes, and other encryption.[129] Whether this is a personal choice, or one imposed by corporate policy, the reality is that a majority of users do use some method

[126] *See* Michael Arnold, *Collecting Data from Mobile Devices*, ABA, http://apps.americanbar.org/litigation/litigationnews/trial_skills/110113-tips-collecting-data-mobile-device.html, *archived at* http://perma.cc/EK2D-U27L (last visited Mar. 3, 2015).

[127] *See, e.g., id.*

[128] *See, e.g., id.*

[129] *Mobile Devices*, STAY SMART ONLINE, http://www.staysmartonline.gov.au/mobile_devices, *archived at* http://perma.cc/QW37-DKCC (last visited Mar. 3, 2015).

to protect the data on their device.[130] These methods can create challenges, delay, or—in some circumstances—prevent inspection and collection of a mobile device.[131] Collection tools such as Cellebrite and Oxygen support decryption, though an uncooperative or unavailable user could limit collection options if advanced encryption is used with next generation devices such as the 'black phone' or Apple and Google's most recent operating systems features.[132] It is yet to be seen how the courts will ultimately see matters when someone asserts her right to privacy.[133]

[47] Cooperative owners and users significantly reduce risk related to intentional or unintentional loss of data due to delay or external intervention. Sometimes the owner and a user may not be the same entity,[134] and there could be a conflict where technologies or policies were not centrally managed by the company,[135] or if the user feels that the risks

[130] *See, e.g.*, Donna Tapellini, *Smart Phone Thefts Rose to 3.1 Million Last Year, Consumer Reports Finds*, CONSUMER REPS. (May 28, 2014, 4:00 PM), http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm, *archived at* http://perma.cc/RA4M-J7HP.

[131] *See* AYERS ET AL., *supra* 110, at 43.

[132] *See, e.g.*, James B. Comey, Director, Federal Bureau of Investigation, Remarks at the Brookings Inst. (Oct. 16, 2014), *available at* http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course, *archived at* http://perma.cc/HGK5-UPMV.

[133] *See* Andy Greenberg, *Google and Apple Won't Unlock Your Phone, But a Court Can Make You Do It*, WIRED (Sept. 22, 2014 6:30 AM), http://www.wired.com/2014/09/google-apple-wont-unlock-phone-court-can-make/, *archived at* http://perma.cc/4L8Y-MVDZ.

[134] *See, e.g.*, *Ex-Lawyer Tells Goffer Jury He Traded 3Com Merger Tips for Cash*, BLOOMBERG (May 19, 2011, 12:01 AM), http://www.bloomberg.com/news/2011-05-19/goffer-trial-witness-says-he-traded-merger-tips-for-cash-filled-envelopes.html, *archived at* http://perma.cc/C4AG-S3WR.

[135] *Id.*

associated with lack of cooperation are more favorable than the discovery of information on the mobile device.[136]

[48] Synchronized devices are not limited to just a computer that may periodically back up the device, but may include any device that can remotely change the data on the device even after it is taken into custody.[137] A typical smartphone or tablet will have multiple programs running on it that communicate over a number of networks such as cellular, wireless (Wi-Fi), Bluetooth, and low-frequency near field communications.[138] Through any of these methods, or through remote access or control, data can be altered or even completely removed from a device if not secured properly.[139]

[49] The type of device, its operating system, features, and characteristics can have a significant impact not only on how collection may need to be performed, but also on the steps for preservation at time of securing the device.[140] Apple, Samsung, Microsoft, and Blackberry are some of the major players in the mobile device marketspace; however,

---

[136] *See, e.g.*, Sentencing Memorandum on Behalf of Raj Rajaratnam, *United States v. Raj Rajaratnam*, 2011 U.S. Dist. LEXIS 21062, at 59 (S.D.N.Y. Aug. 9, 2011), *available at* http://www.law.du.edu/documents/corporate-governance/criminal/rajaratnam/Sentencing-Memorandum-on-Behalf-of-Raj-Rajaratnam-US-v-Rajaratnam-S1-09-CR-1184-SD-NY-August-9-2011.pdf, *archived at* http://perma.cc/ZKA7-D5F7.

[137] *See, e.g.*, Arnold, *supra* note 126.

[138] Gonzalez, *supra* note 125.

[139] *See, e.g.*, Rene Millman, *Smartphones & Tablets Remotely Wiped in UK Police Custody*, ITPRO (Oct. 10, 2014), http://www.itpro.co.uk/security/23273/smartphones-tablets-remotely-wiped-in-uk-police-custody, *archived at* http://perma.cc/4TE6-TVKH; Jane Wakefield, *Devices Being Remotely Wiped in Police Custody*, BBC NEWS (Oct. 9, 2014, 8:30 AM), http://www.bbc.com/news/technology-29464889, *archived at* http://perma.cc/RZS6-29KX.

[140] *See* Arnold, *supra* note 126.

Google, HP, LG, and others have 'smart' mobile devices with different operating systems, operating system versions, features, power sources, and connectors.[141] Sometimes the simplest design feature such an easily removable battery[142] can impact the timing of the preservation of data or accessing simple information like serial numbers.[143]

[50] It should also be mentioned here that security tools and applications must constantly be adapted to account for the constantly changing and ever expanding market of mobile devices.[144] The skills for preserving, inspecting, collecting and interpreting mobile data must constantly be honed and even the results of tested tools must be validated and confirmed to maintain the most accurate and defensible presentation of data.[145]

[51] The nature of the litigation or cause for collection is very important and should be a starting point for considering how one may need to approach a collection, and even then everything may not align in your favor.

---

[141] *See, e.g.*, Jessica Dolcourt, *Best Phones of 2015*, CNET (Feb. 20, 2015, 11:16 AM), http://www.cnet.com/topics/phones/best-phones/, *archived at* http://perma.cc/KR96-B6PH; *see also* Thomas Halleck, *Google Planning Two Nexus Smartphones for 2015: Rumor Pegs LG For New Nexus 6* (Mar. 2, 2015, 7:53 PM), http://www.ibtimes.com/google-planning-two-nexus-smartphones-2015-rumor-pegs-lg-new-nexus-6-1833718, *archived at* http://perma.cc/87EN-RUWD.

[142] *See, e.g.*, *How to Remove the Battery from an iPhone*, WIKIHOW, http://www.wikihow.com/Remove-the-Battery-from-an-iPhone, *archived at* http://perma.cc/7BED-EHFA (last visited Jan. 28, 2015) (noting nine steps are needed to remove the iPhone 5 battery).

[143] *See* AYERS ET AL., *supra* note 110, at 41.

[144] *See* SOUPPAYA & SCARFONE, *supra* note 121, at 12.

[145] *See* Murphy, *supra* note 71, at 9.

[52] For typical commercial litigation, where the information sought is related to typical business documents, communications (e.g., e-mail and text messages) and data from managed applications, and the device is managed by a corporate MDM system and policy, collection may be somewhat simplified.[146]

[53] Collection gets more complicated in criminal and certain civil litigation where the use of the mobile device is itself part of the issue, or where specific and detailed analysis of the behaviors of a user or actions need to be performed.[147]

[54] Collection may be merited, even when not specifically requested or implicated, in an effort to provide context or justification. For example, in a personal injury claim where a litigant is seeking damages for future loss of ability and fitness, tracking applications could provide historical evidence of actual activities or a decline since injury.[148]

A. Challenges and Complications

[55] In some cases, it may be enough to perform a forensically sound logical collection of select targeted information. Sometimes these collections may not even involve the actual mobile device when a reliable current backup or synchronized source of data is available.[149]

---

[146] *See, e.g.*, CDW, MOBILE DEVICE MANAGEMENT: NOT WHAT IT USED TO BE 4 (2012), *available at* http://webobjects.cdw.com/webobjects/media/pdf/108281-WP-Mobile-Device-Mgt.pdf, *archived at* http://perma.cc/KHT6-D8TK; *see also* Arnold, *supra* note 126.

[147] *See* Arnold, *supra* note 126.

[148] *See* Parmy Olsen, *Fitbit Data Now Being Used In The Courtroom*, FORBES (Nov. 11, 2014, 4:10 PM), http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/, *archived at* http://perma.cc/MFG8-CCVV.

[149] *See* Arnold, *supra* note 126.

[56] In both criminal and many civil cases today, mobile data and even just the evidence of use of a mobile device may be important and may necessitate a more comprehensive evaluation of devices and sources outside of the primary device.[150] Criminals are becoming more tech-savvy, with many learning how to hide, encrypt, and even destroy their data on demand.[151]

1. Cooperation and Privacy

[57] Of course, complications will arise even in simple cases when the user is not cooperative, cannot locate the device, or is subject to other governing privacy regulations such as EU Directive 94/46/EC which, in short, is founded on seven basic principles:

- **Notice**: subjects whose data is being collected should be given notice of such collection.
- **Purpose**: data collected should be used only for stated purpose(s) and for other purpose.
- **Consent**: personal data should not be disclosed or shared with third parties without consent from its subject(s).
- **Security**: once collected, personal data should be kept safe and secure from potential abuse, theft, or loss.
- **Disclosure**: subjects whose personal data is being collected should be informed as to the party or parties collecting such data.
- **Access**: subjects should granted access to their personal data and allowed to correct any inaccuracies.
- **Accountability**: subjects should be able to hold personal data collectors accountable for adhering to all seven of

[150] *See id.*

[151] *See* Tim Crushing, *DOJ Whines That A Warrant To Search A Mobile Phone Makes It More Difficult To Catch Criminals*, TECHDIRT (Apr. 24, 2014, 12:48 PM), https://www.techdirt.com/articles/20140423/15081827008/government-argues-that-warrant-requirement-cell-phone-searches-does-nothing-keep-cops-catching-bad-guys.shtml, *archived at* https://perma.cc/8UDA-EXDY.

these principles.[152]

2. Ownership Challenges

[58] Even with cooperative users or companies, there can be complications when the two are not one and the same, and there are differing viewpoints.

[59] In 2013, Gartner predicted that by 2017 one half of employers will require employees to supply their own device.[153] At the moment, thirty-eight percent of employees in mature markets—such as the US—like to use a single device for both work and personal use,[154] and as much as 46% of companies either ignore or are not aware of the use of personal devices for business use.[155] The convenience of using a personal device for both personal and business purposes becomes a problem when users are told that they need to give up their personal device and allow it to be inspected and potentially collected in whole as an image vs. targeted collections.[156]

---

[152] *See Protection of personal data*, EUROPEAN COMMISSION (Apr. 9, 2014), *available at* http://ec.europa.eu/justice/data-protection/, *archived at* http://perma.cc/VG4A-RDF9.

[153] *See* Press Release, Gartner, Inc., Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes (May 1, 2013), *available at* http://www.gartner.com/newsroom/id/2466615, *archived at* http://perma.cc/ZV7K-RAYY.

[154] *See* Brian Proffitt, *Worried Workers: BYOD Or You're SOL [Infographic]*, READWRITE (Dec. 6, 2012), http://readwrite.com/2012/12/06/pause-economy-linked-to-bring-your-own-device-use, *archived at* http://perma.cc/Q7X3-RYY9.

[155] *See id.*; *see also Businesses Unprepared to Support New Mobile Ways of Working*, CITRIX (Nov. 21, 2011), http://www.citrix.com/news/announcements/nov-2011/businesses-unprepared-to-support-new-mobile-ways-of-working.html, *archived at* http://perma.cc/7AHJ-ARDP.

[156] Haman Allen & David Herman, *Challenges of Mobile Devices, BYOD and EDiscovery*, LAW TECHNOLOGY TODAY (Sept. 19, 2014), http://www.lawtechnologytoday.org/2014/09/challenges-of-mobile-devices-byod-and-ediscovery/, *archived at* http://perma.cc/4HPP-MDHY.

3. Resources

[60] The actors who preserve, collect, and review mobile device data are very similar to those who work with connected computing devices. However, their skillsets may be very different, and there is an increased importance in the handling and timing of events. Turning mobile devices off does not ensure that data does not get changed, and introduces the potential that pin codes or other authentication may be triggered when turned back on.[157] For example, first responders need to be specially equipped and trained to handle the mobile devices initially.[158] Improperly secured or handled devices could potentially be remotely turned back on, wiped, reloaded, or have data altered through synchronization.[159]

[61] Properly trained forensic experts and first responders must be prepared with the skills and tools to act quickly and effectively, whether through the use of radio shielding solutions like a Faraday container to prevent external influence, creating a clone UICC card (e.g. SIM, USIM, RUIM or CSIM) without the ability to communicate with a cellular network, disabling wireless, or preserving the usable state of the device.[160] Observations and inquiry must be performed early in the securing of a mobile device.[161] If a mobile device is unlocked and undamaged, has sufficient power or the owner is willing and able to supply any authentication codes, a logical collection might be possible quickly and

[157] *See* Gonzalez, *supra* note 125.

[158] *See* AYERS ET AL., *supra* note 110, at 27.

[159] *See* Arnold, *supra* note 126.

[160] *See* AYERS ET AL., *supra* note 110, at 29.

[161] *See* Jill Griset & Melissa Laws, *Navigating A Case Through E-discovery*, MCGUIRE WOODS LLP 2 (2012), http://www.mcguirewoods.com/news-resources/publications/navigating-e-discovery.pdf, *archived at* http://perma.cc/C4A7-LBW8.

without additional costs.[162] When devices have authentication codes that are unknown, encryption is enabled or the device is physically damaged, costs and time for collection can go up substantially even for a device with limited in-device memory.[163]

[62] Problematically, there may be a backlog to qualified data extraction facilities or engineers, which can result in the loss or destruction of data through delays before collection.[164]

III. CONCLUSION

[63] Mobile data is unavoidable in modern discovery and will continue to play an increasingly significant role in litigation. Beyond the devices that are the subject of this discussion, the market experiences new innovations almost daily, including new "wearable" technology and the Internet of Things, all of which will be sources of potentially relevant information under the right circumstances.[165]

[64] Attorneys must be prepared to assess and evaluate each new source of information based on the capabilities of the technology and the needs of the case. The legal standard will remain constant: reasonableness given the issues at stake in the litigation. But this is merely the starting point for the legal decisions about collection, which must be informed by the cost

[162] *See* AYERS ET AL., *supra* note 110, at 35–37; DIGITAL MOUNTAIN, INC, TAKING THE FIRST STEP—DATA PRESERVATION 2 (2009), *available at* http://digitalmountain.com/fullaccess/Article5.pdf, *archived at* http://perma.cc/S77J-UEXF.

[163] *See* Arnold, *supra* note 126.

[164] *See* Millman, *supra* note 90.

[165] *See* Ted Samson, *How Wearable Tech Will Fuel The Internet of Things*, INFOWORLD (June 5, 2013), http://www.infoworld.com/article/2614798/mobile-technology/how-wearable-tech-will-fuel-the-internet-of-things.html, *archived at* http://perma.cc/3DBN-CWHY.

and complexity of the activity balanced against the need for the information at issue. Whatever the collection method, it is important to document each step and every decision in the process to defend against potential challenges.