The Sedona Conference Journal

Volume 18 2017

The Challenge of Collecting Data from Mobile Devices in eDiscovery

Robert D. Keeling

Recommended Citation:

Robert D. Keeling, The Challenge of Collecting Data from Mobile Devices in eDiscovery, 18 Sedona Conf. J. 177 (2017).

For this and additional publications see: https://thesedonaconference.org/publications

The Sedona Conference Journal® (ISSN 1530-4981) is published on an annual or semi-annual basis, containing selections from the preceding year's conferences and Working Group efforts. The Journal is available on a complimentary basis to courthouses and public law libraries and by annual subscription to others ($95; $45 for conference participants and Working Group members). Send us an email (info@sedonaconference.org) or call (1-602-258-4910) to order or for further information. Check our website for further information about our conferences, Working Groups, and publications: www.thesedonaconference.org.

Comments (strongly encouraged) and requests to reproduce all or portions of this issue should be directed to:
The Sedona Conference,
301 East Bethany Home Road, Suite C-297, Phoenix, AZ 85012 or
info@sedonaconference.org or call 1-602-258-4910.

The Sedona Conference Journal® designed by MargoBDesignLLC at www.margobdesign.com or mbraman@sedona.net.

Cite items in this volume to "18 Sedona Conf. J. _____ (2017)."

THE CHALLENGE OF COLLECTING DATA FROM MOBILE DEVICES IN EDISCOVERY

*Robert D. Keeling**

This article has been prepared for informational purposes only and does not constitute legal advice. This information is not intended to create, and the receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers. The views and opinions expressed in this article are those of the author only and do not reflect in any way the views and opinions of any law firm, company, agency, or other entity to which the author is affiliated.

In an increasingly mobile world, we rely ever more heavily on our mobile devices, specifically mobile applications, to both send and store written communications and various information. The ubiquity of such applications makes it inevitable that they will increasingly be a discovery target in nearly all types of litigation. Indeed, text messages, email, and social media postings are already common sources of data requested by litigating parties.[1] But as mobile communication and storage be-

* Robert Keeling is a partner at Sidley Austin and an experienced litigator whose practice includes a special focus on electronic discovery matters. He is co-chair of Sidley's eDiscovery Task Force and represents both plaintiffs and defendants in civil litigation throughout the nation and conducts internal investigations in the U.S. and throughout the world.

1. *See, e.g.*, Smith v. Hillshire Brands, 2014 WL 2804188 (D. Kan. June 20, 2014); Lee v. Stonebridge Life Ins. Co., 2013 WL 3889209 (N.D. Cal. July 30, 2013); The Katiroll Co. v. Kati Roll and Platters, Inc., No. 10-3620, 2011 WL

come more pervasive, mobile applications become more sophisticated in an effort to secure sensitive content. Accordingly, while requests to collect mobile device data may seem facially reasonable, collection often goes well beyond what has traditionally been recovered and is far more difficult and expensive than what recent case law would suggest.

With proportionality the new standard for discovery,[2] the burden to collect mobile device data matters.[3] And, importantly, the evolution of mobile device technology has outpaced opportunities for courts to make informed and reasoned judgments about what is proportional in this area. Because of this, prior precedent governing the discovery of mobile devices frequently becomes outdated after just a few years. Rather than relying on precedent that fails to fully appreciate the increasing complexity of mobile device technology, courts should zero in on the specific burdens associated with extracting mobile device data in each individual case and balance those costs against the importance of the desired data to the merits; only then may courts resolve discovery disputes in a proportional manner.

OVERVIEW

Under former Rule 26(b)(1), the legal standard for discovery was relevance; discovery was generally permitted unless it was clear that the information sought would have no possible bearing on the claim or defense of a party.[4] If a request appeared relevant on its face, the objecting party had the burden of

3583408 (D.N.J. Aug. 3, 2011); Torres v. Lexington Ins. Co., 237 F.R.D. 533 (D.P.R. 2006).

2. *See* FED. R. CIV. P. 26(b)(1).

3. David Crump, *Goodbye "Reasonably Calculated"; You're Replaced by "Proportionality": Deciphering the New Federal Scope of Discovery*, 23 GEO. MASON L. REV. 1093, 1100 (2016).

4. 2014 WL 2804188 (D. Kan. June 20, 2014).

demonstrating the request's nonrelevance.[5] Proportionality, as a check, frequently operated to tailor the collection and production of content to relevance alone.

For example, in *Smith v. Hillshire Brands*,[6] the defendant requested the plaintiff, a former employee, to produce both electronic communications regarding the allegations raised in the complaint and the plaintiff's social networking activity.[7] The judge in *Smith* granted the defendant's first request, but limited the defendant's second request to *relevant* social media activity, *i.e.*, postings that directly referenced matters in the complaint, the defendant more generally, or events that could reasonably be expected to produce a significant emotional or mental state.[8] The approach in *Smith* is emblematic of how most courts handled requests for electronically stored information (ESI) and social media data.[9]

Notably missing from the relevancy discussion that predominates/characterizes the law governing discovery and production of ESI on mobile devices, however, is the technological complexity associated with communications made via secure mobile messenger applications, which make it more burdensome to extract and collect than unsecured cloud data or even traditional email correspondence. But two recent developments come together to require, going forward, that the technological complexity of mobile device data be a critical and threshold

5. *Id.*

6. *Id.*

7. *Id.* at *1.

8. *Hillshire Brands*, 2014 WL 2804188, at *3–6. *See also*, *e.g.*, Ogden v. All-State Career Sch., 299 F.R.D. 446, 448–50 (W.D. Pa. 2014); Giacchetto v. Patchogue-Medford Union Free Sch. Dist., 293 F.R.D. 112, 115–16 (E.D.N.Y. 2013).

9. Crump, *supra* note 3, at 1094–96.

component in disputes over the scope of electronic discovery (eDiscovery).

First, the Federal Rules of Civil Procedure were amended in 2015 to make proportionality a condition on the *scope* of discovery, as opposed to an extrinsic limitation.[10] The revision impacts what is considered discoverable in a dispute, but it remains unclear how courts will apply the new standard to ESI or mobile device data.[11] The Sedona Conference, however, has determined that a proper proportionality analysis must consider six overarching principles: (1) the burden and cost of preserving relevant ESI as against the data's uniqueness and value; (2) whether there are more convenient and less expensive sources of information; (3) whether any undue burden, expense, or delay results from a party's action or inaction; (4) the need for concrete information versus speculation regarding the data's value and the burden to produce it; (5) what nonmonetary factors restrict the parties' behavior; and (6) other available technologies to reduce the costs to collect and produce.[12]

Second, the mobile application industry has grown exponentially in size, scope, and sophistication. Between 2015 and 2016, the annual gross revenue of the mobile application industry grew by $3.6 billion in the Americas.[13] It is estimated that in four

10. FED. R. CIV. P. 26(b)(1) (2015) advisory committee's note.

11. Crump, *supra* note 3, at 1104–05; *see also* Moore v. Lowe's Home Ctrs., LLC, 2016 WL 687111, at *5 (W.D. Wash. Feb. 19, 2016) (holding that a secondary search of emails with eighty-eight terms was "not proportional," but without explaining how).

12. The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 18 SEDONA CONF. J. 141, 146 (2017).

13. Dean Takahashi, *The app economy could double to $101 billion by 2020*, VENTUREBEAT (Feb. 10, 2016, 6:00 AM), http://venturebeat.com/2016/02/10/the-app-economy-could-double-to-101b-by-2020-research-firm-says/.

years, the industry's gross domestic revenue will be approximately $26 billion,[14] making it bigger than the entire global music business in 2015.[15] Mobile applications have propelled our devices beyond a simple phone into a miniaturized, all-purpose life tool. They permit users to have immediate and more varied methods of communication, keep up to date on sports and current events, manage finances, listen to music, and play games.

Many mobile applications utilize cloud databases, and service providers allow for remote access to networks and data storage via Internet connection anytime and anywhere. For discovery purposes, cloud data is readily available to users, and courts easily may require production of information in that cloud.[16] However, cloud networks are also widely perceived to be insecure.[17] Consequently, users have sought out applications and networks that provide additional security for their private communications, such as WhatsApp (the most used messaging

14. *Id.*

15. Glen Peoples, *This $25 Billion Global Music Industry Isn't Everything*, BILLBOARD (Dec. 11, 2015), http://www.billboard.com/articles/business/6805318/25-billion-global-music-industry-not-everything.

16. Robert Keeling, *How To Avoid Discovery Problems While Using the Cloud*, LAW360 (Mar. 7, 2014), http://www.sidley.com/~/media/files/publications/2014/03/how-to-avoid-discovery-problems-while-using-the-__/files/view-article/fileattachment/law360_how-to-avoid-discovery-problems-while-usi__.pdf. *See also*, *e.g.*, Mt. Hawley Ins. Co. v. Felman Prod., Inc., 269 F.R.D. 609, 618 (S.D.W. Va. 2010).

17. *See* Bruce Byfield, *Is cloud storage innately insecure?*, LINUX MAGAZINE (Sept. 5, 2014), http://www.linux-magazine.com/Online/Blogs/Off-the-Beat-Bruce-Byfield-s-Blog/Is-cloud-storage-innately-insecure; John Brodkin, *Gartner: Seven cloud-computing security risks*, INFOWORLD (July 2, 2008), http://www.infoworld.com/article/2652198/security/gartner—seven-cloud-computing-security-risks.html. The cloud's perception of insecurity may not be entirely fair. That issue, however, is beyond the scope of this paper.

application in the world), ChatSecure, KakaoTalk, and, more recently, iMessage and Face Time.[18] Most of these applications are built with end-to-end encryption, which means that the service provider itself cannot see the messages that pass between communicating users.[19] While attractive to security-conscience users, the technology necessary to secure those private communications also creates headaches for litigants who must now grapple with that same technology when responding to a discovery request.

NEW CHALLENGES OF COLLECTING DATA FROM PHONES AND APPLICATIONS

The foremost challenge of collecting mobile device data is that it is both costly and time consuming, especially if the device to be proliferated is a smart phone (iPhone, Android, etc.), which is more often than not the case. While some data can easily be extracted using a device's SIM card, other data cannot be retrieved absent the use of new mobile forensics technology. Because mobile device applications often require multiple tools to extract, isolate, process, verify, and then report back on the data,[20] acquisition has become increasingly complex and challenging. Depending on the data, extraction may require commands in the internal server via data cable, putting a boot loader

18. Andra Zaharia, *The Best Encrypted Messaging Apps You Can (and Should) Use Today*, HEIMDAL SECURITY (June 9, 2016), https://heimdalsecurity.com/blog/the-best-encrypted-messaging-apps/. Apple is now especially trusted by many because of the fact that it refused to unlock and decrypt the iPhone of the San Bernardino terrorist. *Id.*

19. Martin Kleppmann, *The Investigatory Powers Bill would increase cybercrime*, MARTIN KLEPPMANN (Nov. 10, 2015), https://martin.kleppmann.com/2015/11/10/investigatory-powers-bill.html.

20. Cynthia A. Murphy, *Cellular Phone Evidence: Data Extraction and Documentation*, https://digital-forensics.sans.org/media/mobile-device-forensic-process-v3.pdf (last visited Feb. 10, 2017).

into the phone that dumps the memory, or even using an electron microscope.[21] Isolating the data (keeping it offline and undetected by other networks) requires effectively "cloning" a SIM card.[22] The technology necessary to accomplish the entire task is highly advanced, and, correspondingly, both expensive and time-intensive.

The two largest providers of data collection service are Cellebrite and Oxygen Forensics.[23] Each company provides forensic extractors that allow users to bypass locks and recover mobile data, including any messages, geographical coordinates, video calls, as well as data that has been deleted.[24] Built for any kind of phone technology, forensic extractors also decode encrypted data, create their own clouds, and then generate reports of the retrieved data. Because the services are custom to the needs of the individual party and matter, the cost can range from $1,000 to over $1 million.[25]

The resource-intensive nature of mobile data extraction underscores the importance of courts conducting a proper proportionality analysis when it comes to requests for such data. In the past, courts have frequently tied proportionality to scope by

---

21. *Id.*

22. *Id.*

23. *Cellebrite Competitive Analysis*, OWLER, https://www.owler.com/iaApp/107565/cellebrite-competitors?onBoardingComplete=true.

24. *See Oxygen Forensic Extractor*, OXYGEN FORENSICS, https://www.oxygen-forensic.com/en/products/oxygen-forensic-extractor (last visited Feb. 10, 2017); Paul Henry, *Quick Look – Cellebrite UFED Using Extract Phone Data & File System Dump*, SANS DIGITAL FORENSICS AND INCIDENT RESPONSE BLOG (Sept. 22, 2010), https://digital-forensics.sans.org/blog/2010/09/22/digital-forensics-quick-cellebrite-ufed-extract-phone-data-file-system-dump/.

25. Cellebrite and other data extraction companies do not publicly display these prices due to their high, subjective variance. As such, this information comes from an unknown sales associate.

narrowing the set of would-be-collected data to that which is strictly relevant. The cost and resources associated with mobile data extraction, however, make this approach somewhat untenable. Even assuming litigants can isolate the mobile application(s) containing the relevant information, depending on the application used, data security or encryption may render extraction and collection of just one application insurmountable. Moreover, unlike data that can be culled prior to extraction or collection, identification of the specific content that warrants collection can only occur after the difficult process of unlocking and extracting that data.

While mobile device data may seem relevant in the abstract, whether it is discoverable in the first instance now requires a careful proportionality analysis that balances the costs of collection and extraction against the value and uniqueness of the mobile data, bearing in mind the nature and value of the litigants' claims and whether the information can be sourced elsewhere.

In recent years, federal judges have sometimes required *objecting* parties to submit affidavits or evidence for why a specific discovery request is overbroad or unduly burdensome, or to at least give an informed estimate as to the nature of that burden.[26] While the 2015 Amendments "do[] not change the existing responsibilities of the court and the parties to consider proportionality . . . [or] place on the party seeking discovery the burden of addressing all proportionality considerations,"[27] given the likely lopsided effect of incorporating mobile forensics technology

26. *See* Ashford v. City of Milwaukee, 304 F.R.D. 547, 553–54 (E.D. Wis. 2015); Gross v. Lunduski, 304 F.R.D. 136, 151 (W.D.N.Y. 2014); Heller v. City of Dallas, 303 F.R.D. 466, 490 (N.D. Tex. 2014); Ehrlich v. Union Pac. R.R. Co., 302 F.R.D. 620, 626 (D. Kan. 2014). *See also* FED. R. CIV. P. 34(b)(2)(C) (2015) advisory committee's note.

27. FED. R. CIV. P. 26(b) (2015) advisory committee's note.

and services into eDiscovery, judges should interpret the proportionality requirement as imposing a burden upon parties requesting mobile device data to show that the request is appropriately narrow and sensitive to those costs.[28] Factors for consideration could include the uniqueness and importance of the mobile device data, the likely location of the data on the device, and whether the information can be gleaned from a less burdensome source. The requirement does, after all, primarily pertain to the *requests* that parties make of one another.

CONCLUSION

As mobile devices have become an everyday source of communication and information-storage, users have demanded applications that ensure the safety of those communications and information. A concomitant consequence of this trend is that mobile device data is becoming increasingly difficult and costly to extract and collect. The growth of technology in this field has outpaced the courts' ability to consider the burdens that are now associated with collection of mobile device data, particularly in light of the new proportionality requirement. Accordingly, prior precedent concerning what is "proportional" may be of limited help with respect to mobile device data going forward. Separately, while courts have always enjoyed the discretion to limit discovery on grounds of proportionality on the back-end, they now have an obligation to incorporate proportionality into the question of what is discoverable in the first instance. This change in scope argues in favor of requests for mobile device discovery that are consistent with the Sedona Conference principles and are also narrowly tailored to the costs and inherent difficulties of data collection.

---

28. FED. R. CIV. P. 26(b)(1) ("Parties may obtain discovery regarding any nonprivileged matter that is . . . proportional to the needs of the case . . . .").