How to Find and Use Smartphone Data

William M. Davis Bovis Kyle Burch & Medlin LLC

I once met an interesting person at a party who told me a story about a difficult breakup which prompted her to cease communications with her former suitor by "blocking" him on various social media apps. She was later surprised to find that he was still able to message her by sending her one dollar via Venmo (a payment service that lets users send and receive money) and typing a message in the comment section. If you've ever used Venmo or PayPal, you're probably as surprised as I was by this story. Most of us think of those apps exclusively as a media for exchanging money—not as a messaging service.

This story says something about the myriad ways we are communicating on smartphones these days. Once upon a time, it was appropriate to think of text messaging and phone calls as one thing and social media as another, but nowadays most traditional social media offer messaging applications that look and feel like traditional text messaging. In fact, most of these messaging applications allow users to make voice/video calls to other users. Nowadays, it's hard to define exactly what a "phone call" is. Is it the transmission of voice data across a network that generates a CDR (call detail record) reported on a mobile phone bill—or is it a call on Facebook, WhatsApp, Signal or a similar messaging service that bypasses a carrier's phone network and is reported only as "data usage" on a mobile phone bill?

It's no secret that smartphone data—including social media and messaging—can be relevant in multiple legal contexts. Smartphone data has been used to show wrongdoing and regulatory violations in the securities industry. Smartphone users have sued employers over BYOD (bring your own device) policies which involve monitoring employee communications in violation of federal and state privacy laws.

Most commonly, smartphone data is of interest to parties to litigation, as such data can establish precise communication timelines, maps of locations visited by users and even offer a window into physical activity.

If smartphone data is important to the outcome of litigation, then knowing where to look, how to look and how to reduce the data found to admissible evidence is a vital skill for investigators, claims professionals and litigators. In this article, I will discuss some of the most overlooked aspects of smartphone data discovery and use.

LOCAL VERSUS "CLOUD" DATA

Anytime a smartphone is connected to the internet—either through the carrier's cellular network or through a Wi-Fi connection—it has the ability to send and receive data from remote computers. These computers constitute what is colloquially called "the cloud." Some smartphone data is saved

in the cloud, and other data is saved on the phone itself in its internal storage.

This technical aspect of data storage is important because smartphone data is rarely "lost." A party who lost her smartphone is not locked out of her social media/messaging accounts, as those accounts may be accessed from any internet-enabled device. Likewise, a party who has permanently deleted his social media/messaging accounts may still access his data locally on the internal storage of his smartphone, or the data may be accessed by professionals with special tools.

PUBLIC VERSUS "PRIVATE" DATA

Social media sites allow users to set various privacy settings. A user may appear to the general public to have a minimal social media presence but may actually be sharing significant content daily with thousands of users behind a privacy wall.

Text messages of all sorts are generally thought of as "private" in that they have a limited audience. Text messaging applications are part of every social media service and are colloquially referred to as PMs (private messages) or DMs (direct messages).

Courts have generally not supported a blanket right to privacy of smartphone data—even when users have taken steps to protect privacy. The discovery process should be used to establish the existence of non-public data and to request its production.

SMS, NETWORK CDRS, AND INTERNET DATA

A carrier's cell phone network is a private network, which is different from a generic internet connection through Wi-Fi. Communications occurring over a generic internet connection will not appear as detailed records on the user's monthly phone bills. For example, users who make voice/video calls or send text messages over Facebook, Instagram, Signal, WhatsApp, *etc.* will not see these incoming/outgoing calls and messages appear as detailed records on their phone bills. A smartphone bill showing zero phone calls and zero texts does not mean that the owner of the phone wasn't using it to text and make calls daily over the internet. Conversely, someone who has no social media presence but who texts via SMS (over the carrier network via "regular" text) or makes calls using the carrier network will have a phone bill with detailed entries showing CDRs (call detail records) for each SMS that was sent/received and each call that was made/received. Discovery of smartphone data should thus involve an inspection of phone records and discovery requests targeted to the data on the phone and/or in the cloud.

METADATA

Metadata are data about data. An easy way to think of metadata is to envision a file folder on a computer that contains several files. The files can be sorted by name, date, size, *etc.* Those attributes (filename, size, date created, date modified) are metadata—they are data stored along with the content of the file that describe what the file is, when it was created, *etc.* Metadata are created without any special user input and can be crucial to show the date and time that communications were sent/received. Smartphone data should be considered incomplete without associated metadata.

COLLECTION STRATEGIES

If it is anticipated that smartphone data will be relevant to litigation, a good practice is to send a letter requesting the preservation of the data and the smartphone itself.

Smartphone data can be changed, altered, or hidden through privacy settings, so it is essential efforts to locate and preserve data take place as quickly as possible. If the data is publicly visible (such as a public Facebook page or Instagram account), the data can be downloaded and logged on a continual basis. There are third-party services that will monitor and collect public data on a real-time basis. For non-public data, the collection will depend upon the user disclosing the data pursuant to a proper discovery request. If appropriate, consider a physical inspection of the user's phone by a professional. Such an inspection can be obtained through the agreement of the parties or by obtaining a discovery order from the court.

TAILORED DISCOVERY REQUESTS

Courts have varying opinions regarding the production of smartphone data, but generally speaking, there should be some connection between the data sought and the issues in the pending litigation. Generally, courts will find that requests seeking unlimited discovery of data are overbroad. Limiting discovery requests to specific time periods and connecting them to facts alleged in the litigation or damages sought is a good practice.

WHY SUBPOENAS WON'T WORK

A subpoena will not yield successful results when seeking social media/messaging data directly from a provider. The Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, contains restrictions on the production of certain electronic communications in response to a subpoena. Jurisprudence nationwide generally supports the notion that social media providers are subject to the SCA and are exempt from producing user data in response to a subpoena.

However, it is important to note that most social media providers have developed elaborate preservation tools that the account holder may use to preserve and download his or her entire account. If you have one or more social media accounts, I encourage you to download your own data and see what is available. Typically, you will find the download to contain an astonishing collection of information dating back to the time your account was created. Such data downloads can be searched using keywords to produce relevant results, similar to what is often done in large-scale electronic discovery for corporations.

USE AS EVIDENCE

Courts will require that smartphone data meet the standards for admissibility, meaning that there is sufficient proof of the authenticity of the data and sufficient grounds to establish that the data is not hearsay. Support for authenticity and hearsay exceptions must be generated throughout the discovery process, either by eliciting deposition testimony of the creator of the data, using metadata to establish authenticity, or obtaining the testimony of a recipient of the data.

One good feature of metadata is that it cannot be hearsay because it is not an oral or written statement or nonverbal conduct by a person. Thus, timestamps on messages, GPS tagging of photos, and other aspects of smartphone data are not hearsay. The text of smartphone communications is typically exempt from hearsay if they were written by a party to the litigation.

Not all of your cases are likely to involve jilted lovers who resort to Venmo payments to resume social media communications, but many of them are likely to implicate some form of electronic communications across the vast array of messaging platforms in use today. The best practice is to stay current on the smartphone communications platforms that are widely used and ask for preservation and discovery of any potentially relevant evidence early in litigation.

Billy Davis defends businesses and professionals against a variety of contract and tort claims, including commercial trucking/transportation, professional negligence, premises liability, industrial accidents, products liability, catastrophic accidents, contractual obligations and insurance coverage.