

Mobile Device Forensics: A Brave New World?

Contributed by Jason Gonzalez and James Hung, Stroz Friedberg LLC

Say your client is charged with trade secret theft. What if you could show electronic evidence that, at the time of the theft, your client was in a Starbucks miles away from the crime scene? Or driving down the freeway, talking on his mobile phone? Or sending mundane text messages to his spouse? Or taking photos at the beach? If this sounds appealing, you need to learn about mobile device forensics.

Mobile devices – cell phones, BlackBerrys, Androids, iPads – are everywhere. People use them to take photographs, send texts and emails, update Facebook, consult maps, search the web – the list goes on. As they do this, however, their mobile devices often are quietly making records and generating evidence of those activities. For better or for worse, this makes mobile devices perhaps the richest source of evidence about the people that use them.

Obtaining and using this evidence, however, can present some challenges. Just like mobile device technology itself, the process of obtaining mobile device evidence, as well as the associated law, is constantly changing. This article is intended to help lawyers navigate these potential challenges.

An Overview of Mobile Device Technology

A good way to think about mobile device forensics is to contrast it with "standard," personal computer

based forensics. In PC-based forensics, the paradigm approach is to physically remove the hard drive from the computer, make and verify a bit-for-bit mirror image of it, and analyze that image using forensic software. Because the vast majority of PCs use Windows or Mac operating systems, the forensic techniques and software tools generally are well-developed and robust.

This paradigm doesn't quite work for mobile devices, at least not yet. The primary problem is that, because the mobile device industry is still relatively young, a multitude of different operating systems, communications protocols, and data storage methods are in use, and more are being developed every day. Here's a brief overview:

Operating Systems: The Windows operating system has dominated the personal computer market for years. While Apple's Mac OS has been making inroads lately, by and large the PC operating system market is fairly mature and stable. The same is not true for mobile devices. Many more operating systems are widely-used, including Apple's iOS, Google's Android, RIM's BlackBerry OS, Microsoft's Windows Mobile, HP's webOS, Nokia's Symbian OS, and many others. This diversity creates challenges for developers of forensic software, and for mobile device forensics in general.

Communications Protocols: Mobile devices communicate primarily through three technologies:

© 2011 Bloomberg Finance L.P. All rights reserved. Originally published by Bloomberg Finance L.P. in the Vol. 3, No. 10 edition of the Bloomberg Law Reports—Technology Law. Reprinted with permission. Bloomberg Law Reports[®] is a registered trademark and service mark of Bloomberg Finance L.P.

This document and any discussions set forth herein are for informational purposes only, and should not be construed as legal advice, which has to be addressed to particular facts and circumstances involved in any given situation. Review or use of the document and any discussions does not create an attorney-client relationship with the author or publisher. To the extent that this document may contain suggested provisions, they will require modification to suit a particular transaction, jurisdiction or situation. Please consult with an attorney with the appropriate level of experience if you have any questions. Any tax information contained in the document or discussions is not intended to be used, and cannot be used, for purposes of avoiding penalties imposed under the United States Internal Revenue Code. Any opinions expressed are those of the author. Bloomberg Finance L.P. and its affiliated entities do not take responsibility for the content in this document or discussions and do not make any representation or warranty as to their completeness or accuracy.

cellular, WiFi, and Bluetooth. Cellular communications involve technology that divides large geographic service areas into smaller areas called cells. Each cell contains a communications device (a "cell site"), usually on a tower, that transmits radio signals to and from mobile devices. There is an alphabet soup of transmission technologies used for these communications, including among others GSM, CDMA, GPRS, EV-DO, EDGE, DECT, TDMA, and iDEN.

WiFi, like cellular, transmits communications by using radio waves, but uses higher frequencies and is generally much faster. WiFi communications travel from the mobile device to a wireless access point, which along with a modem/router decodes the communications and transmits them over the Internet. The access point must be within relatively close physical proximity (usually around 100 feet or less) to the mobile device to receive its WiFi signal, which is transmitted from the device using a variant of the "802.11" networking standard (e.g., 802.11a, 802.11b, and 802.11g).

Bluetooth is a wireless communications technology, but its purpose is somewhat different than cellular or WiFi – it is designed to allow various "paired" devices that are physically close to each other (generally less than 30 feet apart) to seamlessly communicate. In other words, Bluetooth can enable your iPhone to communicate automatically with your audio headset, or your iPad to communicate automatically with your external keyboard.

Data Storage Methods: Mobile devices generally can store information in three locations. One is internal memory. The internal memory on a mobile device consists of its RAM ("Random Access Memory") and its ROM ("Read Only Memory"). In brief, RAM is the memory space that your mobile device can use to temporarily store information when the device is performing tasks. Once the device is powered off, all data in RAM generally is lost. ROM is generally pre-programmed information or instructions embedded onto computer chips, often designed to perform specific discrete tasks.

Mobile devices also store information in SIM ("Subscriber Identity Module") cards and memory cards. Although they look a lot alike, SIM cards and memory cards are not the same. SIM cards are designed primarily to connect (or "authenticate") the device user to the user's cellular network, and store limited data focused primarily on the user's identity. Memory cards provide general-purpose storage capacity that the device can use to store photographs, music, videos, and the like.

Lastly, mobile devices can store information on the various other machines and devices they interact with, including email servers, the servers of cellular service providers (for text messages, among other things), and personal computers.

Mobile Device Forensics

While this technological diversity and constant innovation may be good for consumers, it makes it challenging for the forensic field to keep up. There is not, as of yet, a true "standard" approach to mobile device forensics, and working with a skilled and experienced examiner therefore is an absolute necessity. The mobile device examiner, working with counsel, likely will need to consider:

How to collect the device? This may sound trivial, but this decision can have a significant impact on the type of data you are able to obtain. Because mobile devices can communicate constantly, a very real concern exists that the data you are interested in (especially email, texts, and Internet history) could be crowded out by newly-arriving data and disappear if the device is not rendered incommunicative. This could be as simple as turning the device off, but you should be aware that this could have some unintended consequences. Turning the device off generally will result in the loss of data in RAM memory. It can also activate password protections that, depending on your situation, could make it impossible to access the data. The same effect could happen if the device's batteries run out, which can make it important to collect any cables and chargers.

What analysis will be done? There are many different ways to forensically analyze a mobile device. One technique developed early on is decidedly low-tech: simply manipulating the phone (by navigating through the email, photographs, or contacts list, for example) while videotaping and/or photographing the results. While this may be sufficient for some cases, obvious disadvantages include the fact that it involves manipulating and changing the very evidence you are seeking to preserve. Another technique can involve using the device's own backup or "syncing" application, such as Apple's iTunes backup feature. This technique is relatively easy, and it allows a significant amount of user-created data (photographs, songs, emails, texts) to be preserved. Care must be taken, however, to modify the settings so that data from the "synced" computer does not overwrite the data on the device. Like the first technique, it also involves some manipulation, and thus alteration, of the evidence. A third technique is to use commercially available forensic software tools which, as time passes, are becoming increasingly more capable and sophisticated. This software generally makes a full copy of all the files on the device (i.e., a "logical" copy), which can result in a capture of most user-created data, and even some deleted data. Another technique, considered by some to be the "holy grail" of mobile device forensics, is doing a full physical copy (i.e., all the bits in memory, not just the files) of the entire memory store on the device. This method, which can be very difficult to perform properly, allows deleted files and any data remnants present (i.e., in unallocated memory or file system space) to be examined, which otherwise would go unfound.

Justification and Documentation Whatever collection technique or method of analysis is used, you should be prepared to justify it. As discussed above, some methods of collection and analysis can involve alteration of the underlying data, which may cause authentication and/or admissibility problems in legal proceedings if not handled properly. Ensure that your justification is fully documented at the time the decision is reached.

What Evidence Can You Get?

While mobile device forensics can present many challenges, the potential payoff can be significant. You are fairly well assured of getting the basics, including call logs, texts, contacts, calendar items, multimedia (photos, music, et cetera), memos, notes, and potentially email. You may also be able to retrieve Internet browsing history, screenshots, voicemails, information regarding mobile "apps," (including when they were purchased), videos, map histories, geolocation information (including from coordinates stored in photographs taken by the device), and records of access to wireless networks. More difficult, but generally still possible, is the recovery of deleted information.

While all of this information could be useful in various cases, perhaps the most interesting information – or at least the type of information that sets mobile device evidence apart from traditional PC evidence – is the location data. Many cases could hinge on the location of a particular person at a particular time, and this information may be gleaned from various sources on a mobile device. You may be able to see that, for example, a criminal suspect's mobile device accessed a Google map of the victim's neighborhood on the morning of the crime. Conversely, you may be able to see that at the time of the crime the criminal defendant's mobile device was linked to a particular wireless network (at a Starbucks, let's say) far from the scene of the crime. Or you could see that photos taken on the defendant's mobile device on the day of the crime show that the device (and presumably the defendant) were out of state when the crime occurred; cell site data may be recoverable that could show the same thing.

Legal Issues

Issues can arise with the admissibility of nearly any type of evidence, and evidence from mobile devices is no exception. For purposes of this article, we'll focus on three: (1) collection and preservation; (2) privacy; and (3) reliability.

The method of collection and preservation of mobile device evidence is of paramount significance to its later admissibility, and may have other collateral effects in litigation. For example, many people may believe that, because their servers "sync" or backup their mobile devices, there is no need for mobile devices to be collected and analyzed in litigation. Some litigants have learned the hard way, however, that sometimes syncing or backing up does not in fact capture everything it is supposed to.¹ Also, consider whether data that is not set to be synced – texts, photos, and call logs being potential examples – is relevant to the litigation. Moreover, if you decide to collect the evidence, make sure to do it properly: simply using a tape recorder to preserve a key voicemail, for example, can lead to evidentiary problems, particularly if the other side disputes the authenticity and seeks to forensically examine the original.

Privacy is another significant issue, made worse by the fact that the law regarding the privacy of mobile device data (and computer data in general) is unsettled. Generally, though, the privacy analysis regarding the collection of mobile device evidence may involve a close look at: (1) usage policies and privacy warnings associated with the use of the mobile device; (2) the intrusiveness of the data collection method; and (3) the geographic source of the data.

Courts will look to usage policies and privacy warnings to determine whether the mobile device user (usually at a business or enterprise) has a reasonable expectation of privacy in the data on the device.² For example, if the user has to click through an explicit warning every time she uses the device stating that it cannot be used for personal activity and is subject to monitoring, it is more likely that a court will find that she has no reasonable expectation of privacy. Be warned, however, that some courts have read such warnings and usage policies strictly, construing any ambiguities against the company.³ They also have looked to whether any oral statements from superiors contravened or

"softened" the warnings or policies, effectively overriding them.⁴ The bottom line: if your enterprise has a policy (and it probably should), make sure it is unambiguous, and do your best to ensure that all employees know and follow it.

If you have decided to collect mobile device data, you should carefully consider tailoring the collection method to focus precisely on the data you want: courts often focus on this when determining whether data collections are appropriate.⁵ If certain communications are relevant in your case, for example, you may want to *preserve* all the evidence from the device, but only *review* emails and texts from it. Personnel involved in the preservation of the evidence could even be "walled off" from those that review the emails and texts, to ensure that there can be no claim that irrelevant and/or private information was improperly viewed. If this review, or any other evidence you come across, gives you grounds to believe additional data from the device is relevant, you could present those grounds to the court to justify the review of this additional data.

Lastly, be aware that if the data is from Europe, privacy becomes paramount. European law generally holds that personal information remains private, even if it is contained on a company's computer, device, or network.⁶ Moreover, some European countries have "blocking" statutes, which are laws designed to ensure that discovery, even for suits filed in the United States, occurs only under the supervision of European courts. And several European countries have labor laws that specifically prevent an employer from viewing an employee's private information, even if that information is stored on a corporate network.

The final consideration is reliability – in other words, has your expert collected and analyzed the mobile device evidence in a defensible and reliable manner, so that it can be admitted in court? Because mobile device technology is so diverse and constantly changing, it is entirely possible that a particular forensic technique used in your case may be relatively novel and untested. Combined with

the fact that many of the mobile device forensic techniques involve something less than a full forensic "image" of the device, and can also involve some alteration of the evidence, a fight can easily erupt over whether the evidence should be admitted at all. The work of a skilled forensic examiner, in consultation with counsel, can assuage these concerns.

Conclusion

Mobile devices are everywhere, and contain more evidence about their users than perhaps any other source. The technology is constantly changing, making forensics a challenge. Handled properly, however, a forensic examination of a mobile device can yield evidence that can't be found anywhere else, including communications and geographic location data that can change the course of an entire case or investigation.

Jason Gonzalez is a Managing Director at Stroz Friedberg LLC, a digital risk management and investigations firm specializing in digital forensics, e-discovery, data breach and cybercrime response, and business intelligence and investigations. He is a former federal prosecutor. He may be contacted at jgonzalez@strozfriedberg.com. James Hung is a Digital Forensic Examiner at Stroz Friedberg, and may be reached at jhung@strozfriedberg.com.

implications of emerging technology before its role in society has become clear." *Id.*

³ See, e.g., *Stengart v. Loving Care Agency*, 408 N.J.Super. 54, 63-66 (2010).

⁴ See, e.g., *Quon*, 130 S. Ct. at 2629.

⁵ See, e.g., *United States v. Comprehensive Drug Testing*; 621 F.3d 1162, 1170-72, 1177 (9th Cir. 2010) ("The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect."); *Quon*, 130 S. Ct. at 2631.

⁶ See EU Data Protection Directive 95/46/EC.

¹ *Southeastern Mech. Servs. v. Brody*, 657 F. Supp. 2d 1293 (M.D. Fla 2009) (adverse inference instruction given where defendants "wiped" evidence from their BlackBerrys and company could not recover wiped evidence from company server because the BlackBerrys did not properly sync all relevant email to the company's server, and because relevant items – calendars, texts, call logs – were not set to sync at all).

² See, e.g., *City of Ontario v. Quon*, 130 S. Ct. 2619, 2629 (2010). The Supreme Court also notes in *Quon* that it "must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer" and that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment