BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT



# What Every Foreign Corrupt Practices Act Lawyer Should Know About Mobile Telephone Forensics

*John Reed Stark is Managing Director in charge of the Washington office of Stroz Friedberg, a digital forensics and e-discovery consulting firm. Formerly, Stark served for almost 20 years in the Enforcement Division of the Securities and Exchange Commission, the last 11 of which as Chief of its Office of Internet Enforcement. He also has served for the past 15 years as an adjunct professor of law at the Georgetown University Law Center, where he teaches a course on Technology and the SEC and Advanced Securities Regulation.*

BY JOHN REED STARK

Mobile telephone devices have transformed our lives forever. Whether used merely as a communications gizmo to assist us with the bevy of ordinary personal and professional tasks that crop up during the day, or used as a high-tech viaduct to connect with others in ways beyond mere telephone chatter, cell phones have co-opted our existence and renovated our lifestyles dramatically.

Not surprisingly, concomitant with their explosive growth, the electronically stored information (or "ESI") within the circuitry and periphery of mobile telephone devices has become a primary source of evidence and discovery in investigations and litigation, especially investigations pertaining to the Foreign Corrupt Practices Act (FCPA).[1] However, despite their potential to be-

[1] The U.S. Foreign Corrupt Practices Act of 1977 ("FCPA") generally prohibits U.S. companies and citizens, foreign companies listed on a U.S. stock exchange, or any person acting while in the United States, from corruptly paying or offering to pay, directly or indirectly, money or anything of value to a foreign official to obtain or retain business (the "Antibribery Provisions"). The FCPA also requires "issuers" (any company including foreign companies) with securities traded on a U.S. exchange or otherwise required to file periodic reports with the Securities and Exchange Commission) to keep books and records that accurately reflect business transactions and to maintain effective internal controls. Given the SEC's new specialized FCPA unit; the new whistleblower provisions contained in the Dodd–Frank Wall Street Reform and Consumer

come a smoking gun, FCPA lawyers still often neglect or overlook potentially fruitful evidence residing in the mobile telephone devices of their witnesses. Here's why:

In most instances, neither the Department of Justice (DOJ) nor the Securities and Exchange Commission (SEC), the two federal agencies that share jurisdiction over FCPA violations, can conduct the complex, large scale international investigations almost always required when a potential FCPA violation arises—the investigations are far too labor intensive and typically take place half way around the world. Moreover, the SEC and DOJ surveillance capabilities are too often limited both in scale and capacity for detecting potential FCPA violations (even when tipped off by a whistleblower). The result is that the suspected company itself either learns of the potential violation vis-a-vis its own compliance efforts or is informed of the possible violation by the SEC, DOJ, or other regulatory or law enforcement agency—and then performs its own an internal investigation, typically by hiring a large law firm to lead the always substantial undertaking.

But unlike agents from the FBI, Postal Inspection Service, U.S. Secret Service and other federal investigative agencies, FCPA lawyers do not always have the resources, the capacity or the training to develop evidence gleaned from a mobile telephone device—or the experience to recognize which devices are in-scope (i.e. personal devices, work-related devices or both) and which are potentially protected by privacy laws. This is unfortunate, especially given that the typically personal and individualized information derived from a mobile telephone device might not only provide exculpatory evidence but might also serve as just the kind of evidence needed to convince the SEC or DOJ that an FCPA violation was due more to a rogue employee rather than a systematic failure or breakdown at a company.

To help FCPA lawyers forensically navigate mobile telephone devices, this article offers five important practice points every FCPA lawyer should know about the forensic analysis of mobile telephone devices and the techno-DNA fragments hidden within their casing.

## 1. Identifying the correct make, model and owner.

The term ''cell phone'' probably became antiquated not long after its genesis, because whatever the preferred nomenclature—smart phone, PDA, handheld, etc.—mobile telephone devices possess a vast array of capabilities, and have become more akin to home computers than ordinary telephones. In their early days, the basic list of data found on any given mobile telephone device typically consisted of a call history, phonebook contacts, text messages and perhaps a bit more.

Nowadays, however, in addition to personal notes, calendar events, photos, music, video and other related sources of information, mobile phones can operate an enormous assortment of other programs (commonly referred to as ''apps''), which can warehouse a broad range of ESI potentially relevant to a civil or criminal proceeding or investigation. FCPA lawyers might find this increasingly sizable amount of data not only unique but also potentially very powerful.

But like automobile companies, mobile telephone device makers manufacture many different models which can require different digital diagnostic approaches for their analysis. A consumer can purchase a stripped down, disposable cell phone that provides only the basics (like telephone calling, texting and a generic contact list), or a souped-up smart phone that can do everything except fold its owner's laundry, performing many of the same functions a computer can, albeit on a much smaller scale.

For example, some smartphones encompass the features of cell phones (radio capability) together with the ability to store private data, surf the web, exchange SMS (''short message service'') messages and/or multimedia messages, check mail, instant message (IM), make audio or video calls, download/upload content to and from the internet, take photos, draft documents, edit spreadsheets, compose presentations—the list just goes on and on.

Given all of these complexities and capabilities, unlike typical home computers, the forensic examination of mobile telephone devices does not lend itself to any standard procedural analysis. Rather, each brand/type/model of mobile telephone device can require different methods, tools and/or procedures for the identification and preservation of relevant ESI.

For instance, if the device in question is an iPhone, there exist certain forensic possibilities unique to that device, such as the fact that when an iPhone snaps a high quality photo, it may also record the location of the iPhone when the photo was taken. This geolocation function could prove very useful in a range of scenarios, whether in the context of a murder trial or an insider trading investigation. Additionally, when iPhone users ''sync'' their iPhone with iTunes, the device can create an encrypted or unencrypted back up which contains almost everything on the phone including: contacts, calendar, events, photos, bookmarks, voice memos, etc. in an organized and unobfuscated manner. Successfully harvesting this information not only provides key information but also presents that key information in an organized manner, with a proven methodology.

Thus, before engaging in any mobile phone forensics, the first step for an FCPA lawyer is always to gather an inventory (and the manuals if possible) of the model and capabilities of all mobile telephone devices that could be relevant to an investigation or proceeding—and get the appropriate passcodes. For the examiner, the passcode to access the phone is the most important piece of information. Without the passcode, accessing the phone's data creates unnecessary and potentially insurmountable challenges.

Depending on the make and model of a device, the digital forensics examiner can then begin to craft an approach toward its forensic analysis. But without the specifics, it can be difficult for a forensic examiner to know where to start and can lead to big mistakes at the outset, including corruption, spoliation or destruction of key information.

However, after learning the specifics of a mobile telephone device, bear in mind a glaring privacy related red flag, which is particularly acute for the FCPA lawyer—the issue of ''ownership.'' Who actually ''owns'' a mobile telephone device (e.g. a company or its employee)

---

Protection Act (which reward informants who provide certain types of information leading to successful securities actions, including FCPA actions); a hefty SEC budget increase; and increased SEC-Department of Justice Collaboration, 2011 and beyond will undoubtedly result in an onslaught of FCPA enforcement actions and prosecutions.

  PVLR ISSN 1538-3423

and the data contained therein is not always clear and whether breaking into a cell phone by cracking a password or entering with permission can trigger serious privacy concerns.

For instance, as one of its basic principles, the European Union Data Protection Directive (95/46/EC) prohibits the processing of personal information without, among other things, the notice to and consent of, the data subject. This could arguably include the data on a cell phone even if that cell phone is owned by a person's employer. Moreover, in the United States, whether a user's personal data contained on a company mobile phone is protected is an evolving and arguably unpredictable area of privacy law (no matter what sort of disclaimer a company mandates its employees sign or accept as a condition of employment).[2]

## 2. Retrieving data in a forensically sound manner.

Mobile phone forensics, i.e. the science of recovering data from a mobile telephone device under forensically sound conditions and using forensically accepted methods to retrieve potentially inculpatory or exculpatory electronically stored evidence (ESI), is rapidly becoming a scientific field within itself.

In order to rely on the integrity and the authenticity of evidence derived from a mobile phone, a good forensic examiner will obtain any relevant data in a manner that does not materially alter the source device or data, except to the minimum extent necessary to obtain the evidence. Just like on the hit TV series *CSI*, ironclad collection of mobile telephone ESI is essential to ensuring the admissibility of evidence—one slip up and an entire defense can fall apart. Unlike desktop or laptop forensics, mobile phone forensics can alter some data, so it is extremely important that examiners take notes and logs all action taken during their analysis.

Like a plumber or a brain surgeon, the first and most important choice for a forensic examiner is what tools to use. Typically in the realm of PC or Mac forensics, tool selection is a relatively obvious and straightforward undertaking. The hardware, software and operating systems have become relatively standard and it is merely a matter of selecting the most recent and appropriate forensic applications, such as AccessData's FTK, Guidance Software's EnCase, Technology Pathways' ProDiscover, Dr. Golden Richard III's Scalpel, Brian Carrier's Sleuth Kit and other similarly established digital forensics programs.

However, when conducting the forensic exam of a mobile telephone device, tool selection is not nearly as standardized. Indeed, when conducting a forensic exam upon a mobile telephone device, an examiner may not only have to use different tools (because one tool is not likely to capture all of one device), but the examiner may also have to use multiple preservation methods. Even the cables, power cords and workstations used for mobile phone forensics are often unique for a particular mobile telephone device.

Consider so-called ''unallocated space.''[3] Depending on the type of mobile telephone device, its unallocated space might contain evidence of deleted text messages, e-mail, photos—even voicemail. Unlike that of a PC or a Mac though, the software and hardware of mobile telephone devices have an evolving and less established relationship to each other, which can present unique challenges for a digital forensics examiner. When confronted with this diversity of systems and software, like an iPhone loaded with five hundred apps, FCPA lawyers should plan to work side by side with digital forensic examiners to develop a methodical plan to identify and focus upon the most relevant ESI and to address the technological variants inherent in such an enterprise.

As technology advances, examiners must continuously adapt the manner in which they retrieve ESI from mobile telephone devices, and develop new and advanced procedures to keep up with their most recent iterations. For instance, while there are some methods designed specifically for Android forensics, there is currently a lack of commercial support behind Android forensic software. However, this lack of process has done little to stop forensics examiners from collecting data from phones running Android. Good forensic examin-

[2] *See, e.g. City of Ontario v. Quon*, 560 U.S. ____, 130 S. Ct. 2619 (2010) (9 PVLR 899, 6/21/10) (Holding unanimously that employers can read text messages—including personal ones—sent by workers on their company cell phones if they have reason to believe that workplace rules are being broken. However, the Court seemed to reject a broad right of privacy for employees, noting that it would tread carefully in deciding how far an employer can go in the future. ''Prudence counsels caution,'' Justice Anthony M. Kennedy wrote, arguing that the court should not use the case of a police officer who sends numerous text messages on company equipment to ''establish far-reaching premises that define the existence, and extent, of privacy expectations'' of workers. He continued: ''Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own.'')

[3] The unallocated space or ''file slack'' of a desktop or laptop personal computers typically provide important leads for digital forensic examiners. Here's why: Files saved to the hard drive of a computer are typically described as residing in ''allocated space,'' i.e., space on the hard drive allocated by the operating system. When a user deletes these so-called ''active files'', the files usually do not disappear from the hard drive. Rather, the operating system no longer allocates or saves that hard drive space for the file and simply designates the data to the pc's unallocated (i.e. unused) space. The data actually stays still—the operating system just marks that portion of the drive as usable for other files. Historically, this unused area of a personal computer would need to be constantly overwritten to make room for new data. However, given the typically large size of today's computer hard drives, systems no longer mandate the reuse of previously used space to store new data, so a digital forensic examiner can still often extract file artifacts, such as deleted files, temporary files (created when a user opens a file), file fragments, deleted Internet history and other, albeit disorganized, but readable bits of data. Indeed, evidence gleaned from unallocated space has become so important in the context of litigation that using a ''wiping program'' to render unrecoverable the artifacts from the unallocated space can even draw a discovery sanction from a judge. (*See TR Investors LLC v. Genger*, No. 3994-VCS, 2010 WL 4696062 (Del. Ch. Dec. 9, 2009), where the court found defendant Arie Genger in contempt of court for ''wiping'' the ''unallocated space'' of the hard drive of his work computer and file server in the face of an order that prohibited him from ''tampering with, destroying or in any way disposing of any Company-related documents, books or records.'')

ers enjoy circumnavigating around temporary barriers posed by new technology, and simply start with the basics (identify, preserve and analyze) and venture forward.

Indeed, the fact that a ''generally accepted forensic process'' does not yet exist in the realm of mobile phone forensics, while admittedly posing a challenge for forensic examiners, should not be considered a dealbreaker by the FCPA lawyer. A skilled forensic examiner who carefully develops a sound methodology and carefully documents his or her approach can still create a solid evidentiary foundation despite the lack of any institutional consensus on methodology.

Along these lines, a good FCPA lawyer will take care to discuss these and other potential issues with an examiner and make sure that the examiner develops an effective and meticulous protocol: 1) to preserve as much as possible of the internal memory of the mobile telephone device; 2) to maintain the integrity of all evidence derived from its often complicated and interwoven modules; and 3) to avoid spoliation, corruption or other ESI damage. Given that manufactures often lock portions of memory (which can only be accessed by the cell phone itself), complete preservation may not be possible.

## 3. Discovering deleted data.

''There's dead and there's mostly dead.''[4] Data contained in a mobile telephone device is not nearly as stable as data contained on a home or office computer. Indeed, sometimes a mobile telephone device can even deceive a user into believing that certain data is erased. For instance, when an iPhone user seeks to wipe his or her iPhone clean of data by using the manual restore function, the iPhone's file system may still remain. Moreover, even if a user fully restores the iPhone via iTunes, and in so doing, destroys the file system, a good forensic examiner can potentially piece the system back together. Indeed, this notion holds true for much of the ESI stored on an iPhone—although a user might believe that he or she has removed evidence from the device's memory, key artifacts and remnants of the data may occasionally linger.

For instance, harvesting deleted files from the flash memory or so-called ''unallocated space'' (discussed above in footnote 3) of certain mobile telephone devices, which was traditionally considered impossible, have now increasingly become obtainable, potentially revealing secrets that a user thought he or she erased or destroyed. The bottom line for FCPA lawyers is that nowadays, unless users physically demolish their devices, there is always the possibility of a successful forensic extraction of potentially relevant information.

FCPA lawyers should also bear in mind that data volatility can also cut both ways. On one hand, a text message might remain even if a user has specifically deleted that text message from memory. As noted earlier, when text messages are erased from a mobile device, contrary to what one might think, the texts are not immediately deleted. Instead, the system only marks the texts to be over-written, and the texts remain in the mobile device's memory until enough new information is added to fill that memory.

On the other hand, some systems constantly overwrite ESI in mobile telephone devices and failing, for example, to disable its transmitter, could actually allow the owner of the device to remotely clear its memory and destroy permanently relevant ESI. Consider for example, the systems on some of the more basic cell phones, like the disposable cell phones often used for criminal schemes, which might only store ''logs'' of a small number of the most recent phone calls or text messages. In such situations, by simply bombarding a phone with new calls and new messages, a clever user might destroy relevant ESI. Hence, the longer an FCPA lawyer waits to acquire a cell phone, the more likely its user may either intentionally or unintentionally overwrite (i.e. permanently erase) relevant ESI such as text messages.

Along these lines, once an FCPA lawyer determines a cell phone may be relevant to a proceeding or investigation, he or she should take immediate precautions to prevent transmission to and from the relevant mobile device or risk the loss of potentially key evidence. A sharp FCPA lawyer can even go one step further: users who attempt to wipe their tracks from a mobile device might leave a second set of even more devastating tracks that could serve as the basis for a spoliation claim or even an obstruction charge.

FCPA lawyers should also watch out for problems caused simply by powering down a cell phone the wrong way. Volatile memory (such as ''random access memory'' or RAM, used for instance in most mobile phones) can be lost when a device loses power while non-volatile memory (such as ROM, or ''read only memory'' also used in most mobile phones) is not.

Similarly, accessing or powering up the ''subscriber identity module'' or ''SIM'' card typically found in handheld devices at the wrong point in the forensic process might not only unintentionally wipe data from its memory or trigger a ''password-protect'' lock, it might even reset dates and time stamps of messages—sounding a death knell for a FCPA lawyer's defense.

## 4. Bypassing security.

Most mobile telephone devices come complete with their own padlock—usually in the form of some sort of numeric code, password or other mode of primitive encryption. Nowadays, these padlocks, while certainly effective, can be successfully cracked by a good forensic examiner.

For instance, some of the more ingenious digital forensic firms market their own custom designed process to unbolt the different types of locks used to secure an iPhone. So long as all parties remain mindful of the privacy-related trappings associated with this new form of hacking (see section 1 above), these tools might be ideal for FCPA lawyers. However, always bear in mind that not only can hacking into an iPhone void its warranty, but poorly executed hacking (e.g. too many incorrect password guesses of an iPhone password) can also trigger the wiping of an iPhone's ESI, permanently impairing the authenticity and integrity of any evidence ultimately discovered.

## 5. Considering the host.

Presently and certainly in the future, most mobile telephone devices will also have a technical relationship with a host computer—whether just to back-up an address book or contact list or to manage and store a large

[4] From the film, The Princess Bride, directed by Rob Reiner, based on a novel written by William Goldman and starring Billy Crystal and Andre the Giant.

   ISSN 1538-3423

amount of media (like the video and music files contained on an iPhone). A good FCPA lawyer should therefore consider not only the mobile telephone device as a potential relevant evidence for discovery but all of the ESI contained on the host computer as well. Indeed, the digital forensics performed on the host computer might prove even more valuable than the digital forensics performed on the device itself.

**Conclusion.**

Although the discipline of mobile phone forensics remains in its infancy, the evidentiary value of data extracted, discovered or gleaned from its memory, media, and modules can be as important as a DNA swab in a murder trial. Just consider some stories in the news:

- Because of 300 unearthed and thought-to-be-deleted iPhone text messages and phone logs, constables in Sydney, Australia reportedly dropped five criminal charges, including rape, against a defendant accused of raping the 18 year-old daughter of a neighbor (and were also even ordered to pay the defendant's legal costs);
- Police in Cambridge, Massachusetts arrested a man for running an automobile ''chop shop,'' who insisted he was innocent. However, the police were apparently able to boost their case considerably when forensic examiners discovered that the wallpaper background on his cell phone was a photo of the defendant in the driver's seat of a stolen Ferrari;
- In Bloomington, Illinois, a man was suspected of taking photos of a neighbor's son while fondling himself. Although upon checking the suspect's mobile phone, the police found no specific photos of the neighbor in question, examiners reportedly did discover more disturbing and arguably incriminating photos on the suspect's phone, which assisted the officers in obtaining a confession from the suspect; and
- By working with service providers, Idaho law enforcement officials tracked a specific user's cell phone to within a few feet, bringing to justice a man who had allegedly shot a woman at a Twin Falls Comfort Inn Hotel.

Given the lack of a standard protocol and the growing complexity of mobile telephone devices, careful planning by an FCPA lawyer must precede the forensic analysis of a mobile telephone device. Unfortunately, without proper identification and preservation, there is rarely the option of a ''do-over.''

The best approach for the successful forensic analysis of a mobile telephone device is a partnership-like collaboration between the FCPA lawyer and the forensic team. Delegation without collaboration can lead to ESI denigration, corruption and/or spoliation—a result that not only loses a case but also tarnishes the reputations of everyone involved, especially the FCPA lawyer pleading his or her client's defense to DOJ or the SEC.