Forensic Collection of Cell Phones

Background

As recently as 10 or 15 years ago, owning a cell phone was something of a novelty. By 2011, however, 85 percent of adults in the United States owned a cell phone. And, of those, 42 percent owned smartphones.

By 2011, as many as 26 percent of homes had abandoned landlines in favor of cell phones. This trend shows no sign of slowing down as younger generations – who have never had a landline of their own – establish their own households.

Cell phones are becoming an integral part and a personal record of people's lives. Cell phone owners rely on their devices not only as telephones, but also as cameras (54 percent of users), internet browsers (44 percent), and mobile bankers (18 percent).

Information collected by a cell phone – whether through a business call, a tweet, or the filming of a family event – is recorded and preserved within the phone long after it has been forgotten or even deleted. Forensically, a phone can be a vital tool in establishing liability or non-culpability in a civil case, or demonstrating an individual's guilt or innocence in a criminal case.

Although a cell phone's capacity for data storage may be immense, the way in which a cell phone stores data means that some items may be overwritten fairly quickly. Older phones may only store data for fifty calls before the information is lost.

What is not overwritten becomes a chronicle of the cell phone owner's personal habits and interactions. A cell phone can reveal the identities of the people the owner spoke or texted with, the number of calls and messages, dates and times, and length of communications. The calendar tracks events attended, the browser history reveals a person's interests, and the photographs show a picture story. The longer a person has owned the phone or re-used the SIM card, the more complete the record.

Extracting Evidence from a Cell Phone

Unlike a laptop or a desktop computer, cell phones do not have standard operating systems across all models, thereby making forensic data extraction more difficult. Most cell phones can be read via compatible computer cable, Infra-Red, or Bluetooth, but some older phones and prepaid phones cannot have their data extracted to a computer. The "collection" of these phones needs to be done the old-fashioned way – by making the data appear on the phone's screen and then taking a picture.

15725 SW Greystone Court, Suite 200, Beaverton OR 97006
Office: 503.906.3930 | Fax: 503.906.3931 | Email: info@ibridgellc.com
www.ibridgellc.com

Although a cell phone is like a miniature personal computer in many ways, its components work differently. Cell phones have greater control over access to memory since they are designed for memory conservation. The phone itself is a combination of the handset, the SIM card, and a memory card. With a newer cell phone, information is typically stored directly on the handset. A SIM card is responsible for identifying the subscriber, containing limited information on call records, and retaining a few text messages. If a phone has a memory card, it stores the user's pictures, games, and applications.

Forensic examiners use a number of tools to extract information from cell phones instead of just cracking them open or taking pictures of what is present on the screen. Popular tools include XRY, Lantern, MPE+, Paraben Device Seizure, MobilEdit!, and EnCase. Each has advantages and disadvantages, and no single tool works with all cell phones.

Even after the data has been extracted, the forensic examiner must still manually check the cell phone to ensure the extraction tool did not miss any obvious data. Missing key pieces of data may be a sign that a collection was not complete.

Information that might be extracted includes:

- Serial numbers of SIM card and handset
- Serial number of previous handsets using the same SIM card
- Cell phone's personal settings
- Details of previous calls made, received, and missed, along with corresponding timestamps
- Text messages received and saved, along with corresponding timestamps
- Deleted text messages
- Music, voicemail, and similar files
- Photographs and other media, as well as embedded information pertaining to date and time of creation
- Data from applications stored on the cell phone
- Calendar entries
- Email
- Internet browsing and search history

The risk of improper collection is loss or spoliation of evidence.

15725 SW Greystone Court, Suite 200, Beaverton OR 97006
Office: 503.906.3930 | Fax: 503.906.3931 | Email: info@ibridgellc.com
www.ibridgellc.com

Gaining Evidence from Service Providers

In addition to collecting information from the cell phone itself, information may also be obtained from service providers. Service providers keep detailed records for tax reasons and marketing purposes, and because homeland security laws require communication records to be maintained for at least ninety days (see 18 U.S.C. § 2703) although records may be retained for longer periods. To access this information, non-governmental parties will need the owner's written consent and will often need a subpoena.

Information that a service provider may have retained includes:

- Telephone numbers for each call, and additional detailed information if the party is registered with the service provider
- Date and time the call began and ended
- Time at which a text was sent and received
- IP addresses assigned to the device
- Cell tower history (which can help track the movement of the phone)
- Paid bills

Retention Periods of Some Major Providers

	Verizon	AT&T	Sprint	T-Mobile
Call Logs	1 year	5-7 years	2+ years	2+ years
Texts	3-5 days	Not retained	Not retained	Not retained
Text Details	1 year	5-7 years	2 years	2 years
IP Session Information	1+ years	3 days	60 days	Not retained
IP Destination Information	90 days	3 days	60 days	Not retained
Bill Copies	3-5 years	5-7 years	7 years	Not retained
Cell Tower History	1 year	3+ years	18-24 months	4-6 months

-U.S. Department of Justice, 2010

It is important to know what might be recovered from a service provider, because information can sometimes be retained longer than within the cell phone and the information cannot be destroyed by the cell phone account holder. These records can also provide a unique perspective regarding the cell phone user's habits, such as special purchases posted to the bill and call records going back many years beyond the user's current cell phone.

15725 SW Greystone Court, Suite 200, Beaverton OR 97006
Office: 503.906.3930 | Fax: 503.906.3931 | Email: info@ibridgellc.com
www.ibridgellc.com

Securing Evidence

During an investigation, the cell phone should be secured as early as possible. Any delay increases the risk that evidence could be lost or destroyed. Cell phones have a limited amount of memory, service providers only keep records for so long, and the cell phone's custodian could potentially damage the phone beyond the point that data will be recoverable. Upon securing the phone, a chain of custody (COC) document needs to be created to detail all recovery steps taken and to track the phone as it changes custodians. Any known passwords should also be recorded in this document.

For many people, a cell phone is an indispensable belonging, and the owner should be reassured that forensic analysis will be completed in a timely manner, that the phone will be returned as soon as possible (sometimes within several hours or less), and that the phone will not be damaged. And, information is not only collected from cell phones within the other party's custody or control, a party will often want to preserve the information on cell phones within that party's custody or control.

Recommendations

- To ensure a safe, efficient, and defensible collection, a procedure should be established before the cell phone is secured.
- Secure the cell phone at the first opportunity.
- Turn off the cell phone to prevent regularly scheduled network updates that may overwrite evidence.
- The cell phone should be secured for transport so that it will not be damaged or accidentally turned on.
- Fully charge the cell phone. Allowing the battery to completely discharge may result in the loss of date, time and other information.
- Establish a chain of custody (COC) document to track the forensic analysis process and any custodian changes.
- Obtain any passwords (e.g., passwords for lock screen or voicemail).
- Establish the identity of the cell phone's registered owner.
- Establish a history of cell phone ownership.
- Determine if any further collection is necessary, such as from other cell phones or from service providers.

In an increasingly digital world, more and more evidence lies within cell phones. It is important to collect this information correctly and defensibly, because even one mistake can lead to the spoliation of evidence and a lost or significantly weakened case.

15725 SW Greystone Court, Suite 200, Beaverton OR 97006
Office: 503.906.3930 | Fax: 503.906.3931 | Email: info@ibridgellc.com
www.ibridgellc.com