© Blue Planet Studio | stock.adobe.com

Cellphone Forensics

What data can be obtained from cellphones, cloud accounts, and network operators? How can this data be used or challenged in court? A cellphone and associated records provide access to a wealth of information about its user. With the right tools and procedures, data can be obtained that provide a complete profile of its user with evidence to either incriminate or exonerate the defendant in a criminal case.

For law enforcement officers to obtain data from the phone, cloud accounts or the network operators, they must have a proper search warrant. In the landmark case *Riley v. California*,[1] the U.S. Supreme Court unanimously held that the warrantless search and seizure of digital contents of a cellphone during an arrest is unconstitutional.

Three categories of data can be obtained from a cellphone account. All can be obtained with a search warrant or subpoena.

1. Data stored on the phone (text, voicemails, pictures, location timeline, documents, contacts, call history, web search history, etc.)

2. Data stored by the cellphone operator (call detail, billing, location, IP addresses, cell towers, etc.)

3. Data stored in the phone Cloud accounts (iCloud, Google Drive, Tinder, Facebook, etc.)

Accessing and Extracting Cellphone Information

Methods of Phone Security

Before a technician can extract data from a phone, he or she has to get past the security protection. In many cases the user of the phone willingly provides access, but in some cases the phone security needs to be bypassed through other methods.

Several software tools are available that can crack passwords and extract data from a phone. However, newer phone models have more difficult security protections and are harder to crack. A device used by law enforcement can crack an iPhone's four-digit PIN in less than 13 minutes. The device can take up to 22.2 hours to crack a six-digit PIN and 92 days to crack an eight-digit PIN. It bypasses the iPhone feature of data wiping the phone after 10 unsuccessful attempts.[2]

Facial recognition is another method to secure a phone. Most studies conclude that this method has serious faults and can be bypassed easily with either a photograph or a 3D rendering of an image. One method used a pair of modified glasses to bypass facial recognition on an iPhone in less than two minutes.[3]

Drawing a pattern that connects a sequence of dots is another method of security. This method has vulnerabilities as well. In some cases, one can see the smudge pattern on the screen. Also, studies show that people casually observing someone drawing his or her pattern have an extremely high success rate of being able to repeat the pattern.[4]

Fingerprints are also vulnerable to attacks. Studies have shown that fake fingerprints can

BY RICHARD MILETIC

bypass authentication at an 80 percent success rate.[5]

The most secure authentication method is a random password of 10 alphanumeric characters or more. This would take many years for today's computers to bypass.

Extracting Data From the Phone

Extracting data typically consists of connecting a computer directly to the hardware port on the phone and running a predefined set of commands that extract an image of the phone memory.

A number of products provide reporting capabilities, keyword searches, image searches, contact relationships, and many other features that allow the user to perform efficient analysis of the data. In some cases, even data that has been deleted by the user can be recovered.

Several types of data relevant to legal proceedings can be extracted from a phone:

- Subscriber and equipment identifiers: IMEI, MEID/ESN (international mobile equipment identity, mobile equipment identifier/electronic serial number)
- Web search terms, bookmarks, and browsing history
- Location information
- Accessed Wi-Fi networks with connected time and date
- Sync and backup information
- Contacts
- Installed applications and usage activity
- User account information including social media
- Photos with location tags
- Voicemail recordings
- Audio files
- Documents
- Videos
- Call history
- Text (SMS) or iMessage chats
- Archived and deleted data

© Scanrail | stock.adobe.com

A longer PIN is safer than a shorter PIN. A four-digit PIN has 10,000 possible variations, but law enforcement can figure it out in 13 minutes. A six-digit PIN has one million possible codes and requires 22 hours to crack.

- Calendar events with time, date, notes, etc.
- Saved passwords — email, web
- Cloud backup logs
- Notes and tasks
- Health data with location if enabled

With this information one can get a complete picture of the phone user's activity, associates, location, and communications. Phone data extraction and analysis software allows one to search contacts, messages, photos, browsing history, and search terms by keyword. A list of contacts having the most communication with the phone user can be reported. All data is time-stamped with UTC or local time.

Information Stored in the Cellphone's Cloud Accounts

For Android and Apple phones, Google and Apple store a vast amount of information in Google Drive and Apple iCloud. This data can be obtained through a search warrant or subpoena.

The following is a list of data relevant to legal proceedings that can be extracted from cloud accounts:

- Complete phone backup
- Account information
- Contacts
- Location timeline possibly going back multiple years
- Text and messaging including message content
- Files such as photos, videos, documents
- Email
- Activity
- Calendar
- Purchases
- Lists, notes, and tasks
- Voicemails and voice messages
- Search history and bookmarks

The cellphone is typically set to perform automatic backups to the cloud account. Even data that has been deleted on the phone may exist in the cloud.

Android phones have a feature called Location Timeline. If this was enabled, the cloud may contain years of location history. Emails and messages are kept in plain text so they can be accessed and read.

Information Stored by the Network Operator

The network operators (e.g., AT&T, T-Mobile, Verizon) store information about the cellphone too. In many cases

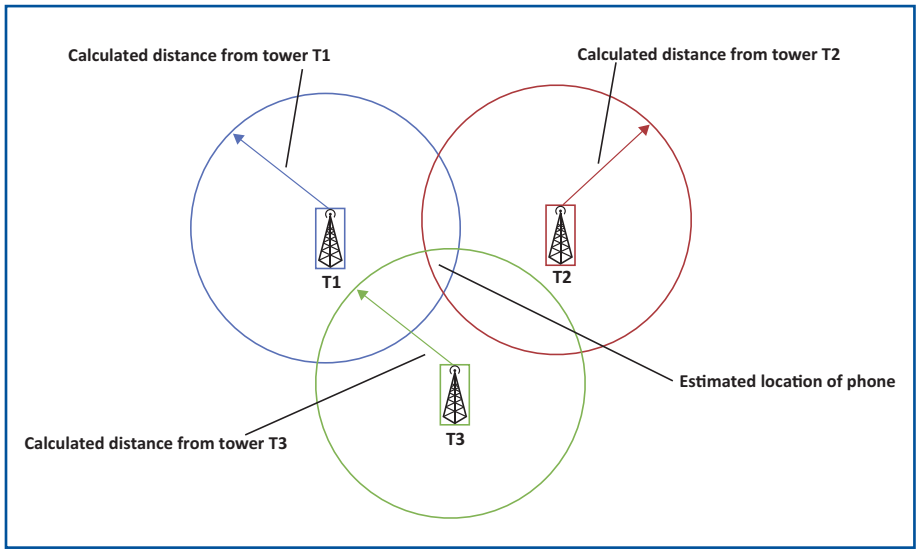

Image courtesy of Richard Miletic

Figure 1. Per Call Measurement Detail (PCMD) records include an estimation of a target phone's location. If three towers communicate with the phone simultaneously, a location estimate can be calculated. The algorithms used to estimate the location are not independently or empirically tested.

this may be the only source of cellphone data available. What is the typical data stored for each cellphone number? How long it is maintained by the network operator?

Account Information

The network operator stores all subscriber information about the account, including account owner, address, payment history, notes, secondary and associated phone numbers, and device Identifiers (including make and model).

Call Detail Record

A Call Detail Record (CDR) is typically stored by the network operator for several years. The CDR will include, but is not limited to, the following:

- Voice Call: Date, time, elapsed time, originating number, terminating number, IMEI, IMSI, call type, feature type, cell ID, cell sector, cell location
- Data (internet communication): Date, time, elapsed time, IMEI, IMSI, cell ID, cell sector, cell location, IP addresses
- SMS (text message): Date, time, originating number, terminating number, IMEI, IMSI, call type, feature type, cell ID, cell sector, cell location

Since the CDR is stored by the operator for multiple years, it is nearly always provided by the network operator in legal cases. Thus, it is the main information used to provide the time and general location of the target phone and the towers serving the phone. The CDR does not provide the location of the target phone, only the location of the cell tower and sector serving the target phone. It also does not provide the geographical signal coverage of the cell tower sector. The coverage of a cell tower sector can range from a few hundred feet to several miles depending on the network design.

In some cases, the prosecution arbitrarily draws a circle or arc showing the coverage area of the cell tower or sector. This is incorrect and misleading, and it was challenged in *United States v. Evans*.[6] In *Evans*, the court determined that estimating coverage areas was unreliable.

Per Call Measurement Detail

The Per Call Measurement Detail (PCMD) records are called "NELOS" for AT&T, "RTT" for Verizon, and "TrueCall" for T-Mobile. These record files are only stored for at most a few months and sometimes just a few weeks before the network operator discards them. It is important to request this data immediately after the event if it will help the client's case. These data are used by the network operator to troubleshoot and improve network quality and performance. The intent of these records is not for legal purposes, and the network operators all provide legal disclaimers absolving their liability.

The main difference between the PCMD record and the CDR is that the PCMD includes an estimation of the location of the target phone while the CDR only provides the location of the serving cell tower. Based on event triggers like internet activity, phone calls or text messages, the network performs a location calculation using a technology called "round trip time."

Round trip time is based on the amount of time it takes for data to be sent between the phone and cell tower. Since radio waves travel at the speed of light, the distance traveled can be calculated by multiplying the time it takes for the radio wave to go from the tower to the phone times the speed of light. If three towers communicate with the phone simultaneously, then a location estimate can be calculated. Figure 1 shows a representation of this analysis.

This location calculation represented in Figure 1 *does not* use GPS or E911 technologies. It is important to make sure the jury is not misled to believe it is just like these well-documented technologies. The prosecution will typically show a point on the map for the location of the phone. This can be misleading and may be challenged. The algorithms used to estimate the location are not publicly available and not independently or empirically tested.

The PCMD data provides a location estimate along with an error or confidence factor that is vague and without any value. Displaying the location of the phone on a map using PCMD data may be challenged under Rule 702.[7]

IP Address Information

Some network operators are providing information on IP addresses accessed as well as the amount of data sent to and from the IP address. With this information, a simple internet search of the IP addresses accessed can identify the company that owns that IP address and its location. This could indicate what phone application is being used. If the application used is Facebook Messenger, for example, then a subpoena or warrant can be served to obtain the messaging information.

Some IP address files contain location information of the phone and the towers serving the phone. This can be compared with the CDR and PCMD files to provide more support or to refute those data sets.

Cell Tower Records

It is important to obtain the list of all the cell towers surrounding the event. The cell tower records frequently include the following items for each tower:

- Site number/ID
- Sector ID
- Location address
- Location latitude/longitude
- Antenna azimuth (direction antenna is pointing in degrees where 0 equals due north)
- Antenna beamwidth (angle of coverage in degrees for the sector — i.e., 3-sector cell has 3 120-degree sectors)
- Technology type (i.e., 3G, 4G)
- Equipment vendor

In some cases, the CDR does not provide the location of the cell tower. Thus, the site number in the tower record is matched with the site number in the CDR to display the location of the cell tower on a map.

Even when the CDR *does* provide the cell tower location, there may be other towers near the event that could have served the phone. This may be critical in determining the possible location of the target phone or in challenging the prosecution's determination of the target phone location.

Cellphone Data From Social Media Accounts

Social media sites also store much information about the user. This information can also be obtained with a subpoena or warrant. Facebook stores a long list of information about its users. Here is a summary of the most relevant data:

- Profile Information — User's contact information, information in user profile's About section, user life events, hobbies, and music
- Posts — Posts the user shared on Facebook, posts that are hidden from the user's timeline and posts the user created
- Photos and Videos — Photos and videos the user uploaded and shared
- Comments — Comments the user posted on the user's own posts and other people's posts
- Likes and Reactions — Posts, comments, and pages the user liked or reacted to
- Friends — People the user is connected to on Facebook
- Stories — Photos and videos the user shared to the user's story
- Following and Followers — People, organizations, or businesses the user chooses to see content from, and people who follow the user
- Messages — Messages the user exchanged with other people on Messenger
- Groups — Groups the user belongs to, groups the user manages, and the user's posts and comments within the groups the user belongs to
- Events — User's responses to events and a list of the events the user created
- Pages — Pages the user is the administrator of, and pages the user recommended
- Marketplace — User's activity on Marketplace
- Payment History — A history of payments the user made through Facebook
- Apps and Websites — Apps and websites the user logs into using Facebook
- Trash — Items the user moved to trash
- Search History — A history of the user's searches on Facebook
- Location — Information related to the user's location
- The user's Address Books
- Security and Login Information — A history of the user's logins, logouts, periods of time that the user has been active on Facebook, and the devices used to access Facebook
- Used IP Addresses
- Voice Recording and Transcription — A history of the user's voice recording and transcription on Facebook

A detailed profile of a person can be created with this information. Contents of messages can be read. Web search keywords are available. A list of friends the person connects to most often can be obtained.

Many social media, dating, messaging, and other sites store personal information. Some examples are Tinder, Twitter, What's App, Instagram, Snapchat, TikTok, Tumblr, YouTube, Reddit, and Pinterest. All these sites maintain personal data on their users.

Conclusion

The amount and type of data collected on a cellphone user is changing rapidly and growing exponentially. Software products are making the analysis of the data less time-consuming and simpler. Securing one's data is becoming increasingly difficult even with the latest verification and security technologies. The data that can be accessed and extracted can be used to create a complete and accurate profile of the cellphone user.

With this understanding and the right knowledge and expertise, much of this data and the representation of this data can be disputed and challenged. Most prosecutors use a law enforcement person to analyze and present the cellphone data. The law enforcement officer does not have cellular technology expertise and in many cases displays the data incorrectly, misleading the jury.

It is important to understand the key aspects of the case and to perform

(Continued on page 63)

About the Author

Richard Miletic has been in the wireless field for over 30 years. He testifies as an expert in criminal and civil cases all over the United States. He has a Bachelor of Science in Engineering from the University of Illinois in Urbana, Illinois, and a Master's in Business from DePaul University in Chicago.

Richard Miletic
ZK Services, LLC
847-220-7760
EMAIL rich@zkservices.net
WEBSITE www.zkservices.net

But Fraenkel's willingness to work within the system did not mean he had the slightest respect for it. As he wrote in his 1935 article, "The Point of Illegal Work," given that the system was rigged against his clients he felt free to use even perjured testimony to secure favorable results on behalf of the politically oppressed.

Fraenkel's book *The Dual State* was both a critique of the Nazi legal system and also "a legal justification for opposing the regime." Fraenkel justified resistance to the Nazi state by his interpretation of rational natural law, a theory that enjoyed a history within Germany, but which had been out of favor for more than a century. Perhaps it is a uniquely German quality that would require extensive thought to justify resistance to the Nazis, which never hid its authoritative and murderous intentions. In a piece written in 1941, Fraenkel celebrated the 150th anniversary of the American Bill of Rights, expressing admiration for the United States, its ideals, and the freedoms it bestowed on its citizens. Morris points out that Fraenkel's concept of freedom, however, was consistent with Goethe's admonition, "Only the law is able to give us freedom."

In the end, the Nazis were defeated not by the internal resistance Fraenkel sought to foster but by Germany's disastrous war in the East, Sherman tanks, the Battle of Berlin, and allied boots on the ground. It is doubtful that Churchill, Roosevelt, or Stalin gave much thought to theories of rational natural law before giving the orders to invade on D-Day or to flatten Berlin. Then again, they weren't Germans.

Fraenkel recognized the limits of his resistance, but nonetheless observed, with justification, that the additional years he spent in Germany before emigrating in 1938 had value, writing to a colleague after the war, "The attempt to save whatever there was to save had to be done — some [of us] had to remain in Germany whose presence … could provide those who could not leave some feelings of assurance and of not being abandoned." With these words perhaps the secular Fraenkel was channeling the 2000-year-old Rabbinic instruction, "You are not required to finish your work, yet neither are you permitted to desist from it."

Morris's writing is crisp and at times poetic. His research is extensive. And, as a federal defender with vast courtroom experience, he ably captures the nuances of legal practice. Ernst Fraenkel, a highly moral and brilliant lawyer and intellectual who acted on his deep-seated beliefs at great personal peril, well deserves the attention Morris so ably devotes to him. ■

Cellphone Forensics

(Continued from page 52)

the cellphone data analysis with this understanding. A great deal of data exists. Much time can be wasted if the analysis is not performed correctly, efficiently, and with the understanding of a how cellphone functions within a cellular network.

This is a rapidly changing environment. New technologies and enhancements are coming online each day. Counsel should partner with experts that maintain their knowledge of wireless technologies.

Notes

1. *Riley v. California*, 573 U.S. 373 (2014).

2. *Researcher Estimates GrayKey Can Unlock 6-Digit iPhone Passcode in 11 Hours, Here's How to Protect Yourself*, April 17, 2018, https://appleinsider.com/articles/18/04/17/researcher-estimates-graykey-can-unlock-a-6-digit-iphone-passcode-in-11-hours-heres-how-to-protect-yourself#:~:text=According%20to%20his%20calculations,%20Green%20estimates%20a%20six-digit,strong%2010-digit%20passcodes%20made%20up%20of%20random%20numbers.

3. Davey Winder, *Apple's iPhone FaceID Hacked in Less Than 120 Seconds*, Aug. 10, 2019, https://www.forbes.com/sites/daveywinder/2019/08/10/apples-iphone-faceid-hacked-in-less-than-120-seconds/?sh=447deb8321bc; Blackhat PowerPoint Presentation, https://i.blackhat.com/USA-19/Wednesday/us-19-Chen-Biometric-Authentication-Under-Threat-Liveness-Detection-Hacking.pdf.

4. Andy Greenberg, *Don't Rely on an Unlock Pattern to Secure Your Android Phone*, Sept. 22, 2017, https://www.wired.com/story/android-unlock-pattern-or-pin; Guixin Ye et al., *Cracking Android Pattern Lock in Five Attempts*, Feb. 27, 2017, https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/cracking-android-pattern-lock-five-attempts.

5. https://arstechnica.com/information-technology/2020/04/attackers-can-bypass-fingerprint-authentication-with-an-80-success-rate.

6. *United States v. Evans*, No. 1:10-cr-00747 (N.D. Ill Aug. 29, 2012), https://thejacobslaw.com/wp-content/uploads/2013/06/celltowertrack.pdf.pdf.

7. *Daubert v. Merrell Dow Pharmaceuticals*, Inc. 509 U.S. 579 (1993). ■

The Champion®

The Champion® (ISSN 0744-9488) is published monthly, except for January/February and September/October, which are bimonthly, by the National Association of Criminal Defense Lawyers®, Inc. Printed in the United States of America. Basic subscription rate $65 per year when received as a benefit of NACDL membership. Non-member subscriptions are $100 annually in the U.S. or $125 if mailed outside the U.S. Periodicals postage paid at Washington, DC and additional mailing offices. Postmaster: Send address changes to *The Champion®*, 1660 L Street, NW, 12th Floor, Washington, DC 20036.

The Champion® is published in the interest of the members of the National Association of Criminal Defense Lawyers® to inform and educate the membership and to improve communication within the criminal defense community. See *www.NACDL.org* for details.

Statements and opinions expressed in *The Champion®* are those of the authors and are not necessarily those of the NACDL®. The information contained in *The Champion®* should not be construed as client-specific legal advice.

Publication of advertising does not imply endorsement. All advertising is subject to the approval of the Publisher. Advertiser and advertising agency assume liability for all content (including text, representation, and claims arising therefrom against the publisher).

Absent prior written agreement, material published in *The Champion®* remains the property of the NACDL®. No material, or parts thereof, may be reproduced or used out of context without prior approval of and proper credit to the magazine.