HACKING & TRACKING: CELL PHONES FOR LAWYERS

FRANK SELLERS, *Fort Worth, Texas*
Westfall Sellers
1701 River Run, Suite 801
Fort Worth, Texas 76107
817-928-4222
frank@westfallsellers.com

ROBERT AGUERO, *Murrieta, California*
CTF DataPro, Inc.
29910 Murrieta Hot Springs Rd, Suite G-221
Murrieta, California 92563
866-935-5551 ext 1 – Office
951-399-3505 – Cell
Robert@CTFDataPro.com
www.CTFDataPro.com

WESTON MUMME, *Lubbock, Texas*
Texas Tech University School of Law
Juris Doctor Candidate 2019

State Bar of Texas
44TH ANNUAL
ADVANCED CRIMINAL LAW
July 24, 2018
San Antonio

CHAPTER 36

FRANK SELLERS
WESTFALL SELLERS
1701 RIVER RUN, SUITE 801
FORT WORTH, TEXAS 76107
817-928-4222
frank@westfallsellers.com

BAR ADMISSIONS

United States Supreme Court

United States District Court Northern District of Texas

State Bar of Texas

EDUCATION

Texas Tech University School of Law, Lubbock, Texas J.D., 2011
- Texas Tech Law Review, Articles Editor
- Texas Tech Board of Barristers
- Texas Aggie Bar Association, President

Texas A&M University, College Station, Texas B.S. — Economics, Business, 2008

ASSOCIATIONS AND MEMBERSHIPS

Texas Criminal Defense Lawyer's Association
- Board of Directors, 2014-present
- Co-Chair, DWI Resource Committee, 2015-present

Tarrant County Criminal Defense Lawyer's Association

Lubbock Criminal Defense Lawyer's Association, President, 2015-2016

DUI Defense Lawyer's Association, Founding Member

National Association of Criminal Defense Lawyers

HONORS & AWARDS

AV Rated, Martindale

Rising Star, Thomson Reuters SuperLawyers (2015-present)

Top 40 Under 40, National Trial Lawyers

Founding Member, DUIDLA

INVITED PRESENTATIONS

Armed with the Best Tools: Efficient, Simple, and Successful Uses of Technology in the Courtroom, Unleashing Your Inner Beast: Defending Those Accused, Texas Criminal Defense Lawyers Association, Salado, Texas (April 2018)

Communicating with the 21st Century Jury, Jury Selection & Communicating with Jurors—A Program for the Defense, Center for American and International Law, Plano, Texas (April 2018)

Faculty, 42nd Annual Texas Criminal Trial College, Texas Criminal Defense Lawyers, Huntsville, Texas (March 2018)

Reframing the Issue: Tylenol, Cyanide and the Burden of Proof, Anatomy of a Trial, Texas Criminal Defense Lawyers Association, Houston, Texas (March 2018)

Armed with the Best Tools: Efficient, Simple, and Successful Uses of Technology in the Courtroom, Unleashing Your Inner Beast: Defending Those Accused, Waco, Texas (January 2018)

The Forensics of Social Media, TCDLA 15th Annual Forensic Seminar, Houston, Texas (December 2017)

Social Media Evidence, 10th Annual Jolly Roger Hal Jackson Memorial Criminal Law Seminar, Denton, Texas (December 2017)

Hacking and Tracking: Cell Phones for Lawyers, Criminal Defense Trial Skills Course, Center for American and International Law, Plano, Texas (August 2017)

Using Social Media in Criminal Cases in Texas, Lawline.com (August 2017)

Hacking and Tracking: Cell Phones for Lawyers, Texas Bar CLE 43rd Annual Advanced Criminal Law Course, Houston, Texas (July 2017) (co-presented with Robert Aguero)

Using Technology and Modern Presentation Techniques, Trainer of the Trainers, South Padre Island, Texas (July 2017)

Social Media in the Courtroom, 30th Annual Rusty Duncan Advanced Criminal Law Course, San Antonio, Texas (June 2017)

Jury Selection in a DWI Blood Test Case, 10th Annual DWI Defense Project, Grapevine, Texas (May 2017)

Communicating With the 21st Century Jury, Jury Selection & Communicating with Jurors — A Program for the Defense, Center for American and International Law, Plano, Texas (April 2017)

Social Media in the Courtroom, Prairie Dog Lawyer's Advanced Criminal Law Seminar, Lubbock, Texas (January 2017)

Fundamentals of Jury Selection, Training for Lubbock Private Defender's Office, Lubbock, Texas (December 2016)

Cross Examination of a DWI Arresting Officer, Stu Kinard Advanced DWI Seminar, San Antonio, Texas (Nov. 4, 2016)

Technology in the Courtroom, Beating the Drum for Justice, Laredo, Texas (October 28, 2016)

Social Media in the Courtroom, Criminal Defense Trial Skills Course, Center for American and International Law, Plano, Texas (August 4, 2016)

Social Media in the Courtroom, Texas State Bar Advanced Criminal Law Seminar, Dallas, Texas (July 20, 2016)

DWI Quick & Dirty: How to Defend a Breath Test, Blood Test, or No Test DWI for the True Defense Lawyer, Upholding Justice One Client at a Time, Waco, Texas (April 22, 2016)

Communicating With the 21st Century Jury, Jury Selection and Communicating with Jurors: A Program for the Defense, Center for American and International Law, Plano, Texas (April 8, 2016)

DWI Quick & Dirty: How to Defend a Breath Test, Blood Test, or No Test DWI for the True Defense Lawyer, Upholding Justice One Client at a Time, San Angelo, Texas (Sept. 18, 2015)

How to Better Manage Your Practice In Court and Out, Criminal Defense Trial Skills & Trial Law Program, Center for American and International Law, Plano, Texas (August 6, 2015)

Communicating With the 21st Century Jury, Training Your Defense Team to Win, South Padre Island, Texas (July 10, 2015)

Communicating With the 21st Century Jury, Jury Selection and Communicating with Jurors in Criminal Cases, Center for American and International Law, Plano, Texas (April 10, 2015)

Jury Selection in a DWI Case Demonstration, A Taste of Voir Dire, Houston, Texas (March 6, 2015)

Pretrial Investigations, Training Your Defense Team to Win, Austin, Texas (January 16, 2015)

Opening Statements & Closing Arguments, Trial Strategies that Work, South Padre Island, Texas (July 17, 2014). Click here to view the paper

Winning Opening Statements, Trial Strategies that Work, Tyler, Texas (April 25, 2014)

Jury Selection in DWI with a Blood Test, The Ultimate Voir Dire, Arlington, Texas (September 28, 2013)

Pretrial Investigations, Trial Strategies that Work, Amarillo, Texas (September 20, 2013)

DWI Quick & Dirty: How to Defend a Breath Test, Blood Test, or No Test DWI for the True Defense Lawyer, Gideon's Trumpet Speaker Series, Corpus Christi, Texas (August 9, 2013)

Battling the Breath Test, 32nd Annual Prairie Dog Lawyers Advanced Criminal Law Seminar, Lubbock, Texas (January 11, 2013)

PUBLISHED ARTICLES

Social Media Evidence, *Voice for the Defense* (Sept. 2017)

Winning Opening Statements, *Voice for the Defense* (Nov. 2014)

Winning Opening Statements, *Harris County Criminal Lawyers Association: The Defender* (Oct. 2014)

ROBERT AGUERO

Robert Aguero started his career as a police officer in 1979. He spent 15 years working in law enforcement. Eight of those years were spent as a detective working primarily gang crimes, narcotics and homicides. He was involved in the investigation of over 30 homicides and wrote and executed more than 200 search warrants. After leaving law enforcement he became a private investigator. He is the owner and CEO of CTF DataPro, Inc. He has been in the private sector for more than 20 years. He specializes in cell phone forensics and cell tower data analysis. He has completed more than 500 cell phone forensics/cell tower data analysis cases and has testified as an expert in court more than 50 times. He is currently certified in the Cellebrite UFED (Universal Forensic Extraction Device), the Cellebrite Physical Analyzer, Katana Lantern, Susteen SecureView3 and Mobile Phone Seizure Certification.

I. INTRODUCTION

On May 24, 2017, nationally-recognized criminal procedure scholar, Orin Kerr, published an opinion piece titled *United States v. Wallace is a GPS Case, Not a Cell-Site Case — Here's Why It Matters*.[1] His article faults the Fifth Circuit's then week-old opinion for misunderstanding the technology involved, leading to a misapplication of the controlling legal principles.

> *Wallace*'s holding hinges on the assumption that the government was not obtaining records directly but was instead obtaining records from a third party that had received the information in the ordinary course of business. But I don't think that happened in *Wallace*. Instead, the government's agent accessed the information directly, "pinging" the phone to obtain location information. In response to the ping, the phone would have turned on its GPS receiver, obtained its GPS coordinates, and sent that information to the government. The information the government received was the data collected by the GPS in the phone, not the business records from AT&T about what cell towers were connected to the phone.[2]

This paper seeks to prevent these types of misunderstandings by providing judges and practicing attorneys with a practical guide to cell phone evidence. Part II focuses on the tools available for hacking cell phones and the specific data they are able to extract. Part III then considers the various methods of tracking cell phones and explains how they work. Lastly, Part IV surveys current Fourth Amendment jurisprudence on cell phone data and how attorneys should navigate the process of challenging cell phone evidence.

II. CELL PHONE HACKING

When officers want to access the information *on* a cell phone, they access that information through a process called hacking. Hacking into a cell phone takes several different forms and the various methods of hacking yield different types of data. Generally, law enforcement attempts to hack phones through the use of third party software programs, phone manufacturers, service providers, or the backup files from a parent computer or cloud based storage provider.

A. What Third-Party Tools Can Unlock Phones?

When law enforcement has possession of a cell phone, secured by a passcode, they utilize third-party software programs to unlock the phone, giving them unencumbered access to the phone's data. Once inside, other software programs allow cell phone data to be analyzed efficiently. While many third-party programs are only compatible with a limited number of phones (with newer phones requiring passwords to hack), the sheer amount of programs available allow law enforcement to hack essentially every phone on the market. Some of the most common programs are Cellebrite, Blacklight, XRY, IP Box, and ElcomSoft.

1. Cellebrite

For years, Cellebrite has been the FBI's main resource for hacking into suspects' phones.[3] Originally used for transferring data between cell phones, in 2007 Cellebrite began marketing its tools for "forensics and law enforcement."[4] Over the years, Cellebrite has become the solution for police when passcodes prevent them from accessing a phone's data.[5]

---

[1] Orin Kerr, United States v. Wallace *is a GPS case, not a cell-site cases—here's why it* matters, WASH. POST, (May 24, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/05/24/united-states-v-wallace-is-a-gps-case-not-a-cell-site-case-heres-why-it-matters/?utm_term=.28a2f75fe130; *but see* United States v. Wallace, 885 F.3d 806 (5th Cir. 2018) (The court withdrew its original opinion and issued this substituted opinion amending its holding and removing the quoted portion in Kerr's article.).

[2] Kerr, *supra* note 1.

[3] Jose Pagliery, *Cellebrite is the FBI's go-to phone hacker*, CNN TECH (Apr. 1, 2016, 2:50 PM), http://money.cnn.com/2016/03/31/technology/cellebrite-fbi-phone/.

[4] *Id.*

[5] *Id.*

In the past, when law enforcement officers were unable to hack into a cell phone using Cellebrite, officers would obtain a warrant demanding the phone be unlocked.[6] Uncooperative phone manufacturers such as Apple, however, updated their security settings beginning with iOS 8.0 to prevent everyone, including themselves, from hacking their devices.[7] Despite Apple's attempts to protect customer data, Cellebrite has enhanced its software and is now able to unlock Apple devices utilizing iOS 8.0 as well as more recent operating systems.[8]

Even cell phones utilizing the most recent technology are not immune to Cellebrite.[9] Rumors suggest the Department of Homeland Security successfully hacked an iPhone X in November of 2017, the same month the phone was released.[10] Once a device is hacked, Cellebrite is able to recover text messages, "downloaded emails, third-party application data, geolocation data and system logs."[11] Due to Cellebrite's seemingly limitless capabilities, phone users should always employ the most recent operating systems to help prevent hacking.[12]

2. Blacklight

After gaining access to a cell phone, Blacklight helps law enforcement examine the phone's data. Blacklight permits law enforcement to view data points which are attributed to a cell phone or computer user's actions, facilitating easy searches through large amounts of data. Blacklight analyzes memory files, finds photo and video evidence, and recovers every message from various sources, such as e-mails or text messages.[13] Additionally, Blacklight is able to search phone information that has been backed up to a computer. Blacklight is compatible with a number of devices including Windows, Android, iPhone, and Mac OS X.[14]

3. XRY

Similarly, XRY permits a forensic extraction of data in devices such as smartphones, tablets, modems, music players, and satellite navigation units.[15] XRY allows for extraction from the device's operating system, memory, cloud-based storages, non-standard mobile devices, and provides screenshots along with extractions.[16]

4. IP Box

For older phones, IP Box allows examiners to gain access to iPhones and iPads, even when the user has employed the 10-try limit for passcode entries.[17] Typically, when the 10-try limit is engaged, Apple products will

---

[6] *Id*.

[7] *Id*.

[8] *Id*.

[9] Thomas Fox-Brewster, *The Feds Can Now (Probably) Unlock Every iPhone Model in Existence*, FORBES (Feb. 26, 2018, 10:20 AM), https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/#6c15df6c667a.

[10] *Id*.

[11] *Id*.

[12] *Id*.

[13] *Blacklight*, BLACKBAG TECHNOLOGIES, https://www.blackbagtech.com/software-products/blacklight.html (last visited May 25, 2018).

[14] *Id.*

[15] *XRY–Extract*, MSAB, https://www.msab.com/products/xry/ (last visited May 25, 2018).

[16] *Id.*

[17] AppleInsider Staff, *New 'IP Box' tool bypasses 10-try limit for PINs on older iOS versions, automates brute force attacks*, APPLEINSIDER (Mar. 18, 2015, 6:50 AM), http://appleinsider.com/articles/15/03/18/new-ip-box-tool-bypasses-10-try-limit-for-pins-on-older-ios-versions-automates-brute-force-attacks.

lock up after ten unsuccessful passcode entry attempts.[18] IP Box bypasses this by entering a passcode via USB and then cutting off power to the iOS device before the attempt is documented.[19]

5. ElcomSoft

ElcomSoft uses proprietary and patented algorithms to hack "even the most complex passwords."[20] The software allows law enforcement to access encrypted information within smartphones.[21]

B. Can the Manufacturer Unlock the Phone?

In addition to utilizing third party software to unlock phones, law enforcement frequently requests phone manufacturers to unlock devices. Whether a manufacturer can unlock a phone depends on the type of device and the manufacturer itself. Despite having created the device, the two biggest phone manufacturers, Apple and Samsung, can only unlock their phones under certain circumstances.

1. Apple

For all devices running iOS 8.0 and later, Apple will not perform data extractions because the extraction tools are no longer effective.[22] Encryption keys protect the user's passcode, which Apple does not have.[23] If the device is running on iOS 4 through iOS 7, Apple may extract "SMS, iMessage, MMS, photos, videos, contacts, audio recording, and call history" pursuant to search warrant based on probable cause.[24] However, unless backed up to iCloud, Apple cannot provide calendar entries, e-mail messages, or any third-party app data.[25]

2. Samsung

Because Samsung makes many different versions of their flagship phone, the Galaxy, knowing the specific model number is helpful to determine whether it can be unlocked. Further, it is common for a specific phone to have different model numbers for each carrier who sells it. For example, the Galaxy Note has over 120 different model numbers. Samsung can bypass over seventy-five percent of those models. The model number can be located behind the battery.

C. Once a Passcode has been cracked, what data can be obtained?

Typically, the following information is available:

- SMS and MMS Message content
- WiFi connections
- Internet search history
- E-mails
- Social media activity
- Application usage
- Contacts
- Some cell tower information

---

[18] *See id.*

[19] *Id.*

[20] *About Elcomsoft*, ELCOMSOFT PROACTIVE SOFTWARE, https://www.elcomsoft.com/company.html (last visited May 25, 2018).

[21] *Id.*

[22] *Legal Process Guidelines*, APPLE, https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf (last visited May 25, 2018).

[23] *Id.*

[24] *Id.*

[25] *Id.*

D. Can I obtain text messages from a service provider?

It is unlikely someone will be able to obtain text messages from a service provider such as AT&T, Verizon, or T-Mobile.[26] Most service providers only retain text messages on their servers for a limited period of time. For many, this period is less than a week.[27] Messages are only retained longer if a person uses the provider's cloud storage or backup services.[28]

If available, text messages are considered a "stored communication." Under the Federal Stored Communications Act (SCA), a law enforcement officer may only obtain stored communication information pursuant to a court order, warrant, or a customer's consent.[29] This information may include text messages, e-mails, photographs, call logs, and location information.[30] On the other hand, a subpoena may be used to acquire transactional records, billing records, and account notes, unless they reflect the location of a phone.[31] The subscriber's general account details, such as name, address, phone number, and IP address are considered non-content data, and are also available by subpoena or court order.[32]

E. What data can be obtained from a cell phone's backup to iCloud or its associated parent computer?

iCloud information is only available from Apple pursuant to a search warrant issued upon a showing of probable cause.[33] The following information may be available from iCloud:

- subscriber information, such as name, address, e-mail address, and telephone number;
- mail logs, including incoming and outgoing communication time, date, sender/recipient e-mail addresses;
- e-mail content of e-mail address associated with the account; and
- photo stream docs, calendars, contacts, bookmarks and iOS device backups, which includes generally anything contained on the phone.[34]

III. CELL PHONE TRACKING

While hacking pertains to the information *on* a cell phone, tracking concerns a phone's *location(s)*. A phone can be tracked in a variety of ways, such as through the Global Positioning System (GPS), WiFi networks, cell tower data reports, and the location services within the device. Each of these tracking methods generates distinct types of data that are created using different technologies. Once the tracking information is acquired, the difficulty becomes interpreting it.

---

[26] *But see* Love v. State, No. AP-77, 024, 2016 Tex. Crim. App. LEXIS 1445, (Tex. Crim. App. Dec. 7, 2016) (In *Love*, MetroPCS retained content and provided it to law enforcement. MetroPCS was bought by T-Mobile in 2012, however, and would now be unlikely to recover such information.).

[27] *Law Enforcement Telephone Investigations Resource Guide*, ACLU, https://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_irvine4_irvineca.pdf (last visited May 25, 2018).

[28] *AT&T Messages Backup & Sync*, AT&T, https://www.att.com/shop/apps/backup-sync.html (last visited May 25, 2018) (providing backup of text message content for up to 90 days).

[29] 18 U.S.C. § 2703(c) (2017).

[30] *Id.*

[31] *Id.*; *see Law Enforcement Telephone Investigations Resource Guide*, *supra* note 27.

[32] ELENA CONDES & ROBERT AGUERO, *Global Positioning Systems (GPS), Cell Phones, and Other Tracking Devices*, *in* SCIENTIFIC EVIDENCE AND EXPERT TESTIMONY IN CALIFORNIA: 2016 UPDATE 22 (2015).

[33] *See Legal Process Guidelines, supra* note 22.

[34] *Id.*

A. In What Ways Can a Cell Phone Be Tracked?

There are two sources of tracking information for cell phones: the service provider and the phone itself.[35] Each source, however, obtains information through the same tracking methods: GPS, Wifi networks, cell tower data reports, and the location based services within the device.[36]

1. Global Positioning System

GPS uses a constellation of over thirty satellites, orbiting the earth every twelve hours, to provide longitude, latitude, altitude, and precise time.[37] The thirty-plus satellites orbit the earth in a manner that ensures there are always at least six satellites within sight of almost every location of the Earth's surface.[38] A GPS receiver on the Earth's surface determines position by calculating the distance to three or more GPS satellites through a process called "triangulation."[39] Distance from each satellite is determined by calculating the time it takes for a radio signal to reach the satellite.[40] Taken together, these various measurements provide a GPS receiver's location.

The accuracy with which GPS can locate a user's phone is increasing.[41] The Federal Communications Commission (FCC) requires wireless carriers to provide 911 centers with a phone's location with increasing degrees of precision.[42] The FCC's E911 program requires wireless carriers to give emergency responders a phone's longitude and latitude within a range of 50–300 meters.[43] This range varies depending on the type of technology used.[44]

2. WiFi Connections

Cell phones have unique media access control (MAC) addresses that connect devices to WiFi network sensors or Bluetooth devices.[45] When the WiFi or Bluetooth setting is switched on, the phone sends out probes to connect to the network through its sensor.[46] Once connected, the network can determine the phone's location by calculating the strength of signal.[47] Like GPS information, this data is stored in the phone itself.[48]

Cell phones and other devices can be tracked based on a phone's WiFi connections.[49] Forensic analysts are able to extract the phone's WiFi connection data from the phone to determine where the phone has been.[50] This allows analysts to narrow down where a phone has been during a specific time period.[51]

---

[35] *See* CONDES & AGUERO, *supra* note 32.

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id.* at 3–4.

[42] *Id.*

[43] *Enhanced 911- Wireless Services*, FED. COMMS. COMMISSION, https://www.fcc.gov/general/enhanced-9-1-1-wireless-services (last visited May 25, 2018).

[44] *Id.*

[45] *See* CONDES & AGUERO, *supra* note 32, at 12.

[46] *Id.*

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *See id.*

[51] *Id.*

A large number of WiFi networks may be polled and recorded depending on the device's amount of movement.[52] A phone will even record WiFi networks that it was unable to connect to.[53] Because the number of possible connections can be large, WiFi data does not indicate that a phone was necessarily at a particular location.[54] Accordingly, records should be analyzed with all available data to ensure greater accuracy.[55]

Currently, many retail stores are making use of this technology.[56] Retailers are able to track whether a person actually entered their store or simply walked by, where shoppers are located within a store, whether shoppers stop by a cash register, and how frequently a shopper enters the store.[57] In 2013, Nordstrom tracked this information at seventeen of its stores without a shopper's device ever connecting to their WiFi network.[58]

3. Cell Tower Data Reports

Cell phone location evidence commonly involves historical data. Available historical cell phone records include:

- call detail records (CDRs);
- location information from call measurement data (PCMD);
- real-time tool (RTT) records; and
- network event location services (NELOS) records.[59]

CDRs are the records most frequently obtained from cell phone providers.[60] Typically, CDRs provide the date and time a phone call was made, the phone numbers involved, whether a call was incoming or outgoing, the duration of a call, and the cell tower and sector hit during a call.[61] CDRs are kept six months to five years.[62]

PCMD, RTT and NELOS all use round trip delay data to measure how long a radio signal takes to go from the tower to the handset and back to the tower.[63] These measurements provide a phone's geographic coordinates at a given date and time, but this data is not guaranteed to be accurate.[64] All of these records are usually only kept by the provider for a relatively short time period—ranging from just a few days to one month.[65]

Another method of obtaining historical phone data is through "cell tower dumps."[66] These dumps provide the identity of all phone numbers connected to a particular cell tower during a given time period.[67] Presumably,

---

[52] *See* CONDES & AGUERO, *supra* note 32, at 12.

[53] *See id.*

[54] *Id.*

[55] *Id.*

[56] *Id*.

[57] *Id.*

[58] *Id.*

[59] *Id*. at 7.

[60] *See id.*

[61] *See id.*

[62] *Id*.

[63] *Id.*

[64] *Id.*

[65] *Id.*

[66] *Id*. at 17.

[67] *See id.*

gathering this information requires a warrant or a court order showing probable cause.[68] This method is typically most helpful when law enforcement does not know the suspect's phone number.[69] The tower dump will identify towers in the area surrounding a crime scene and also provide a list of all calls processed by that tower during the relevant time frame.[70] Likewise, defense counsel can request cell tower dump records to help show a defendant's location is consistent with an alibi defense during a key time period.[71]

4. Location Services on Phone

The GPS location shown on phone applications comes from location-based services (LBS), which uses real-time data from a cell phone to track itself.[72] Cell phones rely on assisted GPS (A-GPS) to obtain their location.[73] A-GPS uses the GPS satellites in combination with nearby cell towers to figure out its own position.[74] In addition to GPS and cell towers, LBS can also use WiFi to locate itself.[75] While they be used individually to locate a particular phone, a combination of these three provides the greatest location accuracy .[76]

LBS is used for things like locating stores, proximity-based marketing systems, and providing travel information.[77] Many applications and services that run on electronic devices automatically detect the user's location.[78] This form of live tracking is always done in the background—as long as a phone is turned on.[79] LBS information is generally stored within the phone itself and is not retained by, or transmitted to, the cell phone service providers.[80]

B. How Does a Cell Tower track phones?

A cell tower's main purpose is to raise antennas to transmit and receive radio frequency (RF) signals from cell phones and other devices.[81] Usually, but not always, devices are aware of the nearest tower's location, which is displayed on a device in the form of signal strength. The range of a cell tower can vary from one-quarter mile to twenty-five miles.[82]

Most cell towers contain equipment that allows antennas to receive and transmit RF and GPS signals. A typical cell tower has three sectors—each sector is a set of antennas grouped together to provide directional coverage in

---

[68] *Id.*; *but see* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) ("We do not express a view on matters not before us: real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval).").

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] Daniel Rubino, *GPS v. aGPS: A Quick Tutorial*, WINDOWS CENTRAL (Jan. 3, 2009), https://www.windowscentral.com/gps-vs-agps-quick-tutorial.

[73] *Id.*

[74] *Id.*

[75] *See* CONDES & AGUERO, *supra* note 32, at 5–6.

[76] *Id.*

[77] Ryan Goodrich, *Location-Based Services: Definitions & Examples*, BUS. NEWS DAILY (Oct. 30, 2013, 4:34 PM), http://www.businessnewsdaily.com/5386-location-based-services.html.

[78] *See* CONDES & AGUERO, *supra* note 32, at 5–6.

[79] *Id.*

[80] *Id.*

[81] Michael Harris, *How Cell Towers Work*, UNISON, http://www.unisonsite.com/pdf/resource-center/How%20Towers%20Work.pdf (last visited May 25, 2018).

[82] CONDES & AGUERO, *supra* note 32, at 10.

one direction facing away from the cell tower.[83] The precision of a cell site location depends on the size of the sector. The smaller the sector, the more precise the location information.[84] Sector sizes have steadily been decreasing over time in order to meet demands of dependable cell phone coverage.[85]

These smaller sectors are known as microcells.[86] As of 2010, microcells make up the majority of cell sectors, allowing carriers and analysts to know a phone's location within a shrinking geographical area.[87] Further, some cell phone service providers utilize "time of arrival" and "angle of arrival" enhancements to determine not only the sector in which the phone is located, but also its position within that sector.[88] A cell phone provider can then pinpoint a cell phone's latitude and longitude by correlating the precise time and angle at which a phone's signal arrives at multiple-sector base stations.[89]

But be cautious. If you received NELOS records from AT&T, or PCMD or RTT from any other provider, these records are attempting to locate the phone itself within a particular range, or confidence interval.

C. How May Cell Tower Records Be Obtained?

When cell phone data is material to a case, both opponents and proponents of the data should request copies of all available records. The following information should typically be included in discovery from a cell phone service provider:

- call detail record (CDR) which provides basic call information and cell tower numbers used;
- a cell tower key which provides GPS coordinates for each tower and sector azimuth[90];
- subscriber information which provides the name and address of the subscriber to the phone service and the make and model of the device; and
- a key to reading the records which contains information helpful to understanding the data.[91]

In cases where the FBI analyzed cell tower data, the FBI's Cellular Analyst Survey Team (CAST) prepares a report to assist prosecutors.[92] CAST reports contain information such as: (1) the methodology used in conducting the historical cell site analysis; (2) a mapping of cell tower locations; (3) the orientation of cell sectors for the cell provider's towers; (4) the assumptions in drawing cell sector coverage; and (5) the conclusions regarding cell phone location in cell sites and call patterns in CDRs for text messages and phone calls.[93]

Further, when seeking phone records, knowing the retention time for each service provider is vital. Retention periods for cell phone data differ among service providers and vary from a few days to five years.[94]

---

[83] *Id*. at 12.

[84] *Id*. at 11.

[85] *Id.*

[86] *Id.*

[87] *Id.*

[88] *Id.*

[89] *Id.*

[90] *See id*. at 34 (explaining that the "[a]zimuth is the centerpoint of the sector").

[91] *Id*. at 26.

[92] *Id*. at 27.

[93] *Id.*

[94] *Id*.; *Retention Periods of Major Cellular Service Providers*, ACLU, https://www.aclu.org/files/pdfs/freespeech/retention_periods_of_major_cellular_service_providers.pdf (last visited May 25, 2018).

D. How Do I Read Cell Tower Records?

Reading cell tower records can be a daunting task. To make the process easier, there are a few things to note before you begin. Certainly, an expert can always be hired to read and explain the records to you. However, basic information needed to understand the records should be contained within them.

A key to reading the records should be included, which provides essential information such as the switch information to determine time zones within the records.[95] For example, most of AT&T's older records were reported in the local time zone.[96] Newer records, however, are now reported in the Coordinated Universal Time (UTC), so these records must be adjusted to reflect the local time zone.[97] AT&T's records must also be adjusted for daylight savings time.[98] Further, it is important to use the proper coordinates when studying the data. The carrier provides GPS coordinates for the tower—not the actual location of the phone—for use when examining cell phone location data.[99]

IV. CHALLENGING CELL TOWER AND CELL PHONE EVIDENCE

As the presence of technology in our daily lives increases, so too do the legal questions surrounding cell phone data. Fourth Amendment issues involving law enforcement's ability to search cell phones and cell phone records held by third-parties are becoming more and more common. An in depth understanding of current Forth Amendment jurisprudence is imperative when combating or utilizing cell phone evidence.

The leading case on cell phone privacy is *Riley v. California*. In *Riley*, the arresting officer conducted a warrantless search of the defendant's phone, revealing evidence of unrelated criminal activity.[100] On appeal, the Supreme Court unanimously held an officer must obtain a warrant before searching a phone following an arrest.[101] In doing so, the Court gave a glimpse of how importantly it considers cell phone privacy.

In *Carpenter v. United States*, the Court further illustrated the importance of cell phone privacy when it held the government's acquisition of cell site location information (CSLI) requires a warrant supported by probable cause.[102] In *Carpenter*, the Government sought and obtained court orders for Carpenter's CSLI under the Stored Communications Act (SCA).[103] Prior to his robbery and firearms trial, Carpenter moved to suppress the CSLI evidence, arguing probable cause was required instead of the SCA's lower standard.[104] The Government argued Carpenter lacked a reasonable expectation of privacy in CSLI records because he voluntarily conveyed them to the third-party service provider, who owned the records.[105]

In a 5-4 opinion, Chief Justice Roberts explained CSLI is "qualitatively different" than the dialed phone numbers in *Smith* and the bank records in *Miller*.[106] Rejecting the Government's argument that the records at issue belonged to the third-party service provider—not to Carpenter—the Court said, "Given the unique nature of cell

---

[95] *See* CONDES & AGUERO, *supra* note 32, at 9.

[96] *Id.*

[97] *Id.*

[98] *Id.*

[99] *Id.*

[100] Riley v. California, 134 S. Ct. 2473, 2481 (2014).

[101] *Id*.

[102] Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

[103] *Id*. at 2212.

[104] *Id.*; 18 U.S.C. § 2703(d) (allowing Government court-ordered access to CSLI if it "offers specific and articulable facts showing . . . reasonable grounds to believe" the records sought "are relevant and material to an ongoing criminal investigation").

[105] *Carpenter*, 138 S. Ct. at 2213; Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

[106] *Carpenter*, 138 S. Ct. at 2216–17.

phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[107] "There is a world of difference between the limited types of personal information addressed in Smith and Miller and the exhaustive chronicle of location information casually collected by wireless carriers today. The Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information."[108]

The Court expressly recognized a reasonable expectation of privacy in data which tracks a person's physical movements.[109] For CSLI, "when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user."[110] This is true "[w]hether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier."[111] Individuals maintain "a legitimate expectation of privacy in the record[s] of [their] physical movements as captured through CSLI."[112] Therefore, obtaining location information from wireless carriers is a search.[113]

Carpenter also expressly held court orders under the SCA are not the appropriate way to obtain CSLI. As the Government conceded, under the SCA's standard "law enforcement need only show that the cell-site evidence might be pertinent to an ongoing investigation—a 'gigantic' departure from the probable cause rule[.]"[114] Because government acquisition of CSLI is a search, "the Government's obligation is a familiar one—get a warrant."[115]

The Court concluded:

> We decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection. The Government's acquisition of the cell-site records here was a search under that Amendment.[116]

Justice Gorsuch wrote an independent dissent, offering an increasingly popular property-based perspective to digital data held by third-parties.[117] He would take the third-party doctrine off of "life support," because in his view, *Smith* and *Miller* breed "[a] doubtful application of *Katz* that lets the government search almost whatever it wants whenever it wants."[118]

But to Justice Gorsuch, this problem stems from *Katz* itself.[119] He criticizes the continued use of the *Katz* test, as modified by the third-party doctrine:

> In the end, our lower court colleagues are left with two amorphous balancing tests, a series of weighty and incommensurable principles to consider in them, and a few illustrative examples that seem little more than the product of judicial intuition. In the Court's defense, though, we have

---

[107] *Id*. at 2217.

[108] *Id*. at 2219.

[109] *Id*. at 2217.

[110] *Id*. at 2218.

[111] *Id*. at 2217 (citing United States v. Jones, 565 U.S. 400 (2012)).

[112] *Id*.

[113] *Id*.

[114] *Id*. at 2221 (discussing 18 U.S.C. § 2703).

[115] *Id*.

[116] *Id*. at 2223.

[117] *Id*. at 2261–72 (Gorsuch, J., dissenting).

[118] *Id*. at 2264.

[119] *Id*. at 2267.

> arrived at this strange place not because the Court has misunderstood *Katz*. Far from it. We have arrived here because this is where *Katz* inevitably leads.[120]

Under Justice Gorsuch's property-based approach, "the fact that a third party has access to or possession of" a person's papers and effects does not necessarily eliminate the person's interest in them.[121] Likening digital data to handing a sensitive document to a friend to read, valeting your car, or asking someone to watch your dog while you're out of town, he views a third-party service provider as a bailee who must safely keep your property:

> A bailee normally owes a legal duty to keep the item safe, according to the terms of the parties' contract if they have one, and according to the implication[s] from their conduct if they don't. A bailee who uses the item in a different way than he's supposed to, or against the bailor's instructions, is liable for conversion. This approach is quite different from *Smith* and *Miller*'s (counter)-intuitive approach to reasonable expectations of privacy; where those cases extinguish Fourth Amendment interests once records are given to a third party, property law may preserve them.[122]

Justice Gorsuch suggests looking to positive law for determining whether data is someone's property.[123] He notes in other contexts the Court "often ask[s] whether . . . state-created rights are sufficient to make something someone's property for constitutional purposes."[124] Citing the Texas Property Code, he points out, "Both the States and federal government are actively legislating in the area of third party data storage and the rights users enjoy."[125] To him, the positive law created in state and federal legislatures "may supply a sounder basis for judicial decisionmaking than judicial guesswork about societal expectations."[126]

Under a property-based approach, Justice Gorsuch believes it's "entirely possible a person's cell-site data could qualify as his papers or effects under existing law."[127] Even though in the possession of the provider, "Plainly, customers have substantial legal interests in this information, including at least some right to include, exclude, and control its use. Those interests might even rise to the level of a property right."[128] But because he did not pursue a property-based challenge, in Justice Gorsuch's view, Carpenter forfeited what was "perhaps his most promising line of argument."[129]

Justice Gorsuch's dissent is meant to be a "cautionary tale."[130]

> Unfortunately, too, this case marks the second time this Term that individuals have forfeited Fourth Amendment arguments based on positive law by failing to preserve them.[131] Litigants have had fair notice since at least *United States v. Jones* (2012) and *Florida v. Jardines* (2013) that arguments like these may vindicate Fourth Amendment interests even where *Katz* arguments do not.[132] Still, the arguments have gone unmade, leaving courts to the usual Katz handwaving. These

---

[120] *Id*.

[121] *Id*. at 2268.

[122] *Id*. at 2268–69 (citations and quotation marks omitted).

[123] *Id*. at 2270.

[124] *Id*.

[125] *Id*. (citing 18 U.S.C. § 2701 et seq.; Tex. Prop. Code Ann. § 111.004(12) (West 2017) (defining "[p]roperty" to include "property held in any digital or electronic medium")).

[126] *Id*.

[127] *Id*. at 2272.

[128] *Id*.

[129] *Id*.

[130] *Id*.

[131] *See* Byrd v. United States, 138 S. Ct. 1518, 1526 (2018).

[132] *See* United States v. Jones, 565 U.S. 400 (2012); *see also* Florida v. Jardines, 569 U.S. 1 (2013).

omissions do not serve the development of a sound or fully protective Fourth Amendment jurisprudence.

A. Circuit Views on Cell Site Location Information

Prior to the Supreme Court's *Carpenter* decision, Fourth Amendment jurisprudence from the Fifth and Sixth Circuits suggested law enforcement *may* be allowed to obtain CSLI without a search warrant. In *United States v. Skinner*, the Sixth Circuit held obtaining a suspect's prospective cell site data—data showing a phone's real time location—is not a Fourth Amendment search.[133] The court reasoned when an individual "voluntarily uses a cellular device, he has no reasonable expectation of privacy in the GPS data and location of his cell phone."[134] Similarly, in *United States v. Wallace*, the Fifth Circuit originally held law enforcement officers may use data from cell tower records to track a suspect's phone without a warrant. As noted by Orin Kerr, however, the court mischaracterized *Wallace* as a cell-site case when it was actually a GPS case and would later substitute its opinion correcting the mistake.[135]

In *Wallace*, law enforcement officers used real-time geolocation coordinates obtained from the service provider, through a Ping Order, to find and arrest the defendant.[136] In his motion to suppress, Wallace argued the Ping Order was invalid and the federal pen-trap statute and Texas Code of Criminal Procedure authorizing the Ping Order were unconstitutional.[137] The district court denied the motion, and Wallace was convicted.[138]

On appeal, the Fifth Circuit declined to reach the merits of Wallace's argument stating, "suppression is not a remedy for a violation of either the federal pen-trap statute or the Texas Code of Criminal Procedure."[139] As such, they did not to consider whether obtaining geolocation coordinates of a cell phone constitutes a search within the meaning of the Fourth Amendment.[140] The court did, however, determine that even if suppression was a proper remedy it would not apply in this case because the officers acted in good faith.[141] Essentially, Wallace's substituted opinion created more questions than it resolved. As one justice remarked:

> It is some comfort that, after two revisions, the panel has eliminated several pernicious aspects of its previous opinions. However, the panel's latest revision still misses the mark. It also misses the opportunity to provide sorely needed guidance on the meaning of a complicated and poorly understood statute. Indeed, I am afraid the majority's opinion aggravates rather than alleviates the confusion. For these reasons, I respectfully dissent from the denial of rehearing en banc.[142]

Noting the obvious uncertainty on this issue from the Fifth Circuit, it will be interesting to see how future Fourth Amendment cases turn out post-*Carpenter*.

---

[133] United States v. Skinner, 690 F.3d 772, 781 (6th Cir. 2012).

[134] United States v. Wallace, 857 F.3d 685, 689 (5th Cir. 2017), *withdrawn*, 885 F.3d 806 (5th Cir. 2018), *and reh'g denied en banc*, 885 F.3d 315 (5th Cir. 2018) (alteration omitted) (internal quotation marks omitted) (quoting *Id*.).

[135] *Compare* Kerr, *supra* note 1, *with Id*. at 687 (stating the court order at issue authorized law enforcement to obtain the "locations of cell site towers being accessed by" the defendant), *and* United States v. Wallace, 885 F.3d 806, 808 (5th Cir. 2018), *reh'g denied en banc*, 885 F.3d 315 (5th Cir. 2018) (recharacterizing the information sought by law enforcement as "real-time geolocation coordinates" of the defendant's cell phone).

[136] *Wallace*, 885 F.3d at 808.

[137] *Id*.

[138] *Id*. at 807–09.

[139] *Id*. at 809.

[140] *Id*. at 810.

[141] *Id*. at 810–11.

[142] United States v. Wallace, 885 F.3d 315, 318 (5th Cir. 2018) (Dennis, J., dissenting).

B. Recent Texas Case Law on Cell Site Location Information and Privacy of Cell Phone Data

The Texas Court of Criminal Appeals has contemplated both a person's right to privacy in content-based and non-content-based cell phone data. Its case law indicates content-based records harboring personal information such as text messages, e-mail messages, photographs, and videos, typically warrant Fourth Amendment protection.[143]

In *Love v. State*, the court held a person does in fact have a reasonable expectation of privacy in content-based information, such as text messages.[144] Love was charged with murder, and the State admitted into evidence approximately 1600 of his text messages.[145] Love argued his text messages—obtained by application and court order for text message content from the provider—were obtained in violation of the Constitution.[146] The court agreed, holding "the State was prohibited from compelling Metro PCS to turn over [Love's] content-based communications without first obtaining a warrant supported by probable cause."[147] Because the content-based information was obtained directly from the service provider without a warrant, the evidence should have been excluded.[148]

In *Ford v. State*, the court determined non-content-based cell phone data does not enjoy the same protections.[149] In *Ford*, detectives investigating a murder applied for and received four days' worth of historical CSLI for Ford's phone from AT&T.[150] The records AT&T provided detectives showed the phone was tracked at locations inconsistent with Ford's alibi defense.[151] Based on the phone data and inconsistent alibi testimony, Ford was found guilty of murder.[152] The court ultimately held individuals do not have an expectation of privacy in non-content based information, such as records of a phone's past location, conveyed to a third party.[153] Still, *Ford* gave hope that Art. I, § 9 of the Texas Constitution may provide greater protection than the United States Constitution.[154] That hope was lost, however, when the court decided *Hankston v. State*.[155]

Hankston was convicted of murder. Prior to trial, the State obtained Hankston's cell phone records for the twelve months prior to the offense.[156] Hankston challenged the cell phone records under both the Fourth Amendment and Art. I, § 9 of the Texas Constitution, but the court again held there was no legitimate expectation of privacy in records revealed to a third party.[157] The court further held that Art. I, § 9 of the Texas Constitution and the Fourth Amendment offer the same level of protection, so there is no violation of Art. I, § 9 when law enforcement obtains cell phone records from a third party revealing a phone's location.[158]

---

[143] *See infra* notes 144–148 and accompanying text.

[144] Love v. State, 543 S.W.3d 835, 843 (Tex. Crim. App. 2016).

[145] *Id.* at 839.

[146] *Id.* at 839–40.

[147] *Id.* at 845.

[148] *Id*. at 843–45.

[149] *See* Ford v. State, 477 S.W.3d 321, 330 (Tex. Crim. App. 2015), *cert. denied*, 136 S. Ct. 2380 (2016).

[150] *Id.* at 325.

[151] *Id.* at 326.

[152] *Id*. at 327.

[153] *Id.* at 329; *but see* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

[154] *See Ford*, 477 S.W.3d at n.1.

[155] Hankston v. State, 517 S.W.3d 112 (Tex. Crim. App. 2017), *vacated sub nom*. Hankston v. Texas, No. 17-6213, 2018 WL 3148283 (U.S. June 28, 2018).

[156] *Id.* at 113–14.

[157] *Id.* at 116–20.

[158] *Id.* at 122.

Despite years of Texas caselaw suggesting individuals have little to no expectation of privacy in their cell phone data, cases such as *Riley* and *Carpenter* have breathed new life into the Fourth Amendment. Texas should soon feel the effects of these Supreme Court decisions as leading cases like *Hankston* and *Ford* have already been called into question.[159] Due to their uncertain futures, we should follow these cases closely.

C. Challenging a Warrant or Court Order

The Fourth Amendment does not protect against all searches and seizures, "but only such as are unreasonable."[160] Reasonableness, therefore, is the driving force in any Fourth Amendment analysis.[161] The reasonableness of a search is determined by comparing "the degree to which it intrudes upon an individual's privacy" with "the degree to which it is needed for the promotion of legitimate governmental interests."[162] As technology has advanced, this comparison has become increasingly complex.

1. Which Document is Required?

Under the SCA, a governmental entity, in possession of a valid warrant, may require electronic communication service providers to disclose the contents of a wire or electronic communication.[163] Service providers may also be required to disclose other records related to a particular subscriber pursuant to a warrant or court order.[164] A warrant may be obtained under either the Federal Rules of Criminal Procedure, or State warrant issuing procedures.[165] Obtaining a court order, however, requires "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[166]

2. Probable Cause

For a search warrant to be valid under the Fourth Amendment, it must be based on probable cause.[167] Further, the warrant must describe with particularity the place to be searched and the persons or things to be seized.[168] While there are exceptions to this rule, the purpose of the Fourth Amendment is to protect innocent American citizens against unreasonable searches and seizures.[169]

Probable cause as it relates to cell phones raises new legal questions. The scope of a cell phone search as well as how the search should be executed are still unsettled issues. Pre-*Riley*, when cell phones only performed basic functions, many arresting officers searched cell phones as a "container" upon arrest. However, recent advances in technology make phones look less like containers and more like full file storage rooms. As Chief Justice Roberts remarked, equating a cell phone to a container "is like saying a ride on horseback is materially indistinguishable

---

[159] *See* Hankston v. Texas, No. 17-6213, 2018 WL 3148283 (U.S. June 28, 2018) (vacating the judgment and remanding the case back to the Texas Court of Criminal Appeals just six days after *Carpenter* was decided); *see also* Suggestion for Court to Amend Opinion & Recall Mandate to Prevent an Injustice and Correct the Opinion, Ford v. State, 477 S.W.3d 321 (Tex. Crim. App. 2015) (No. PD-1396-14), *available at* http://www.search.txcourts.gov/SearchMedia.aspx?MediaVersionID=c4813a22-974b-44ef-bc7a-eb9c18901c6d&coa=coscca&DT=LETTER&MediaID=b2287442-231f-4b8b-aeac-46c1dc9f61d8 (requesting the Texas Court of Criminal Appeals rescind mandate and amend opinion to comport with *Carpenter*).

[160] Carroll v. United States, 267 U.S. 132, 147 (1925).

[161] United States v. Knights, 534 U.S. 112, 118 (2001).

[162] Wyoming v. Houghton, 526 U.S. 295, 300 (1999).

[163] 18 U.S.C. § 2703(a) (West 2017).

[164] *Id.* § 2703(c)(1)(A–B).

[165] *Id.* § 2703(c)(1)(A).

[166] *Id.* § 2703(d).

[167] U.S. CONST. amend. IV.

[168] *Id.*

[169] *Id.*

from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together."[170]

3. Nexus

To have probable cause to search a cell phone, many courts have held there must be a nexus connecting the phone and the crime.[171] Probable cause does not exist merely because a law enforcement officer claims it exists. As Chief Justice Roberts wrote in the *Riley* opinion, "[it] would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a phone."[172]

In *State v. Granville*, the Texas Court of Criminal Appeals considered whether a person retains a legitimate expectation of privacy in cell phone contents when his cell phone is being stored in a jail property room.[173] Granville was arrested for the misdemeanor offense of causing a disturbance on a school bus, and while he was detained, his phone was turned on by an officer and searched without a warrant.[174] The officer found a photo that was unrelated to the bus disturbance, and charged Granville with Improper Photography.[175]

The Court ultimately held "a cell phone is not like a pair of pants or a shoe . . . a citizen does not lose his reasonable expectation of privacy in the contents of his cell phone merely because it is being stored in a jail property room."[176] The *Granville* court noted there was no nexus between the offense for which the defendant was jailed and the photos found and seized from the phone.[177] Thus, it is unlikely any probable cause existed to justify a search of the cell phone. Additionally, the Court remarked that even if there was probable cause, a person's cell phone cannot simply be activated and searched without a valid warrant.[178]

4. Overbreadth

A warrant is "overbroad" if it is not supported by probable cause to believe that each of the things law enforcement officers were authorized to search for and seize were evidence of a crime and would be found in the place to be searched.[179] Even post-*Riley*, some courts have upheld overbroad search warrants authorizing searches of electronic data.[180] Warrants that permit general searches of "any and all" data have been found to be valid.[181] Likewise, courts have upheld warrants that do not state a crime for which the evidence is being searched.[182]

For example, in *New York v. Watkins*, an officer obtained a warrant for the video a suspect took on his cell phone as he was being arrested.[183] Upon arrest, the officer frisked Watkins, seized his cell phone, and powered

---

[170] *See* Riley v. California, 134 S. Ct. 2473, 2488 (2014).

[171] *See* Adam M. Gershowitz, *The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 VAND. L. REV. 585, 590 (2016).

[172] *See Riley*, 134 S. Ct. at 2492.

[173] State v. Granville, 423 S.W.3d 399, 402 (Tex. Crim. App. 2014).

[174] *Id.*

[175] *Id.*

[176] *Id.* at 417.

[177] *Id.* at 412.

[178] *Id.* at 417.

[179] *See* People v. Hepner, 21 Cal. App. 4th 761, 773–74, (Cal. Ct. App. 1994).

[180] *See* Gershowitz, *supra* note 171, at 601.

[181] *Id*.

[182] *Id*.

[183] *See* People v. Watkins, 994 N.Y.S.2d 816, 817 (N.Y. Supr. Ct. 2014).

down the device.[184] The officer then sought a search warrant for the entire contents of the phone, even though the video recording could be easily found by the officer. Notably, Watkins did not have the phone back in his possession following the arrest in order to hide any evidence in the phone.[185] There was probable cause to search for the video taken on the phone, but the presiding judge authorized a warrant searching the entire contents of the Watkins's cell phone. The judge reasoned the warrant was not overbroad because it was limited to video, audio, and information relating to the possession of a firearm.[186] Further, the judge asserted that as technology evolves, warrants should be written to reflect "sufficient breadth" to search data of a cell phone in order to determine which file or application has evidentiary value.[187]

5. Particularity

For purposes of the Fourth Amendment, "particularity" refers to the requirement that search warrants must clearly describe the places law enforcement may search, and the property they are permitted to search and subsequently seize.[188] This requirement protects against general search warrants. Law enforcement must describe what they are looking for and where it may be found so they are not aimlessly rummaging through an individual's personal belongings.[189] This requirement "makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another."[190]

To determine whether a warrant is written with sufficient particularity, the Fifth Circuit has asked whether an executing officer reading the warrant would reasonably know what items are to be seized.[191] Where particularity is seemingly impossible, however, they have held a warrant meets the particularity standard if it specifies the types of items to be seized.[192] Concerning digital data, the Fifth Circuit has all but discounted the particularity requirement.

In *United States v. Kimbrough*, Terry Kimbrough was indicted on charges related to child pornography.[193] Agents executed a search warrant for Kimbrough's residence and business and seized a number of items, including computers and computer-related equipment.[194] Kimbrough challenged the search warrants stating that they failed to sufficiently particularize which items could be seized.[195] In relevant part, the warrant permitted seizure of: "[t]apes, cassettes, cartridges, streaming tape, commercial software and manuals, hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media-floppy disks, CD ROMs, tape systems and hard drive, other computer related operational equipment."[196] The court held the *Kimbrough* warrant was sufficiently particular to withstand the defendant's challenge because it limited the executing officers' discretion by informing officers what items may be seized.[197]

The Fifth Circuit has also upheld warrants containing language such as, "assorted pornographic videotapes; assorted pornographic magazines; assorted devices" and "[c]hild pornography; records of victims; drawings;

---

[184] *Id.*

[185] *Id.*

[186] *Id.* at 818.

[187] *Id.*

[188] United States v. Layne, 43 F.3d 127, 132 (5th. Cir. 1995).

[189] *See* Andresen v. Maryland, 427 U.S. 463, 480 (1976).

[190] *See* Marron v. United States, 275 U.S. 192, 196 (1927).

[191] *Layne*, 43 F.3d at 132.

[192] *Id.*

[193] United States v. Kimbrough, 69 F.3d 723, 726 (5th. Cir. 1995).

[194] *Id.*

[195] *Id.* at 727.

[196] *Id.*

[197] *Id.* at 728.

pictures; computer disks, sexual devices; videotapes; child abuse books; magazines; audiotapes; and any other obscene or child pornographic material."[198]

Despite this definitive trend, some egregiously ambiguous warrants have recently been held unconstitutional.[199] In *Washington v. McKee*, the defendant was being investigated for Sexual Exploitation of a Minor.[200] As part of the investigation, law enforcement obtained a warrant for a "physical dump" of the suspects phone.[201] The warrant permitted officers to search the defendant's phone for "[i]mages, video, documents, text messages, contacts, audio recordings, call logs, calendars, notes, tasks, data/internet usage, any and all identifying data, and any other electronic data from the cell phone showing evidence of the above listed crimes."[202] The court criticized the warrant for permitting a search and seizure without regard for whether the information sought was actually related to a crime.[203] Consequently, the court determined the warrant violated the particularity requirement.[204]

The particularity requirement is more vital than ever when considering cell phone data. Permitting law enforcement to perform general searches through cell phones is a major invasion of privacy. Despite the concerns with general searches of cell phone data, courts may be hesitant to rigidly impose the particularity requirement because electronic data can be stored in virtually any place on a cell phone.

Although the Fifth Circuit has yet to address this issue, other circuits have found violations of the particularity requirement when a warrant contains catch-all language and also when the warrant does not state the crime for which a search is being conducted.[205] The Ninth Circuit suggests "[t]he pressing need of law enforcement for broad authorization to examine electronic records . . . creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant."[206]

6. Overbreadth and Particularity

Other federal courts have found warrants simultaneously overbroad and insufficiently particular. In *United States v. Galpin*, the Second Circuit held that a warrant which generally authorized law enforcement to search a defendant's physical property and did not specify a crime for which there was probable cause was overbroad and violated the particularity requirement.[207] Galpin pleaded guilty to several counts relating to the production of child pornography and possession of child pornography.[208] Before his guilty plea, Galpin moved to suppress all evidence, which included digital cameras, images of child pornography found on his computer, and digital storage devices, all of which were seized in the execution of a search warrant.[209] The warrant allowed officers to search for cameras, computers, cell phones, and any and all computing or data processing software "which may reveal evidence which substantiates violations of Penal Law statutes, Corrections Law statutes and or Federal statutes."[210]

The *Galpin* court found the warrant violated the Fourth Amendment's particularity requirement because the only crime specified in the warrant was a sex offender registration offense, and there was no probable cause to

---

[198] United States v. Layne, 43 F.3d 127, 132–33 (5th. Cir. 1995).

[199] State v. McKee, 3 Wn. App. 2d 11, 30 (Wash. Ct. App. 2018).

[200] *Id*. at 25.

[201] *Id*. at 14.

[202] *Id*. at 18.

[203] *Id*. at 29.

[204] *Id.* at 30.

[205] *See* Gershowitz, *supra* note 171, at 599.

[206] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010).

[207] United Sates v. Galpin, 720 F.3d 436, 447 (2d Cir. 2013).

[208] *Id.* at 439.

[209] *Id.*

[210] *Id.* at 441.

believe that Galpin produced or possessed child pornography.[211] Crimes relating to child pornography were not mentioned in the warrant itself or the warrant application.[212] Therefore, the warrant was also overbroad and facially invalid.[213]

Similarly, in *United States v. Zemylanksky*, thirty-six defendants were indicted on various charges in a scheme to defraud automobile insurance companies.[214]A magistrate judge issued a search warrant for six premises, including corporate office buildings.[215] The warrant failed to specify any criminal allegations and listed eight categories of items to be searched and seized.[216] Seven of these categories permitted the seizure of virtually anything that could be found in a billing office, including electronics, passwords, documentation, software, and encryption devices.[217]

The U.S. District Court for the Southern District of New York determined the warrant failed the particularity requirement because the warrant did not limit the search to a criminal offense, included vague and broad terms, and used confusing language which granted executing officers too much discretion.[218] The court further held that the warrant was overbroad because the government lacked probable cause to search and seize all patient care records, bank account information, and patient information within a corporate office.[219] The court also declined to apply the federal good faith exception stating that executing officers acted with at least gross negligence in relying on a facially invalid search warrant.[220]

D. Does the Good Faith Exception Apply?

When the validity of a search warrant is successfully challenged, the general rule provides the unconstitutionally obtained evidence should not be admitted at trial.[221] The so called "good faith exception" outlines key instances where, despite being illegally obtained, evidence may still be used during a prosecutor's case in chief.[222] Currently, courts are grappling with whether the good faith exception should apply to searches of cell phone data.

1. Federal Good Faith Exception

In appropriate situations, the federal exclusionary rule makes inadmissible evidence collected in violation of a defendant's constitutional rights.[223] The federal exclusionary rule states, "all evidence obtained by searches and seizures in violation of the Constitution is … inadmissible in a state court."[224] Later, in *United States v. Leon*, the Supreme Court created the good faith exception, permitting the introduction of evidence obtained on an officer's reasonable belief that the search was executed in compliance with the Constitution.[225] Federal appellate courts have

---

[211] *Id.* at 447.

[212] *Id*.

[213] *Id.*

[214] United States v. Zemylanksky, 945 F. Supp. 2d 438, 444 (S.D.N.Y. 2013).

[215] *Id.* at 451–52.

[216] *Id.* at 454.

[217] *Id.* at 457.

[218] *Id.* at 464.

[219] *Id*. at 465.

[220] *Id.* at 475–76.

[221] *See infra* notes 223–224 and accompanying text.

[222] *See infra* notes 225–226 and accompanying text.

[223] Mapp v. Ohio, 367 U.S. 643, 671 (1961).

[224] *Id.* at 655.

[225] United States v. Leon, 468 U.S. 897, 925 (1984).

applied the good faith exception to evidence from cell phone searches. Recently, states have considered applying their own statutory good faith exception in cases involving cell phone searches.

2. The Fifth Circuit's Application of the Good Faith Exception

In *United States v. Wallace*, the Fifth Circuit reasoned that even if accessing prospective CSLI to obtain a phone's real-time location did constitute a search under the Fourth Amendment, the Special Agent did not have the "knowledge, or [cannot] properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment."[226] The Special Agent in *Wallace* obtained a Ping order to obtain locations of cell site towers the defendant's phone accessed and was able to find the defendant's real-time location based on his GPS location.[227] Wallace argued the Ping order was invalid for a number of reasons, but the court found that the Special Agent had reasonably relied on the text of the statute requiring cell phone providers to turn over records related to its customers, so the Agent did not have knowledge the search was unconstitutional.[228]

3. Article 38.23(b): Texas's Statutory Good Faith Exception

Texas Code of Criminal Procedure art. 38.23(b) codifies the good faith exception to Texas's statutory exclusionary rule.[229] Article 38.23(b) allows evidence obtained using of a defective search warrant to be admitted if the officer was acting in objective good faith reliance on the warrant and the warrant was based on probable cause.[230] This statutory exception to the rule is "somewhat narrower" than the federal rule's exception.[231] According to the statute, the exception applies only when the law enforcement officer acted "in objective good faith reliance upon a warrant issued by a neutral magistrate based on probable cause."[232]

Nevertheless, before Texas courts are able to address the applicability of the good faith exception, they must first determine whether the exclusionary rule even applies in the first place. This is the key issue in *Sims v. State*, currently on discretionary review before the Texas Court of Criminal Appeals.[233] In *Sims*, the defendant was suspected of murdering his grandmother and stealing her vehicle and purse.[234] During pursuit, law enforcement pinged the defendant's cell phone to ascertain his location.[235] The defendant argued the pinging of his cell phone was done in violation of the SCA as well as its Texas counterpart, Texas Code of Criminal Procedure art. 18.21.[236] Accordingly, he requested that all evidence obtained as a result of the warrantless pinging of his phone be excluded under Texas Code of Criminal Procedure art. 38.23(a), the Texas Exclusionary Rule.[237]

---

[226] *Id*. at 919.

[227] United States v. Wallace, 885 F.3d 806, 808 (5th Cir. 2018).

[228] *Id*. at 810–11; Comparably, other circuits have analyzed the exception to Fourth Amendment searches involving other forms of digital data, such as computers files. In *United States v. Otero*, the Tenth Circuit found a warrant obtained to search a computer invalid for lack of particularity, but still permitted the admission of the evidence in applying the good faith exception. United States v. Otero, 563 F.3d 1127, 1136 (10th Cir. 2009). In *United States v. Rosa*, the Second Circuit said that a search of the defendant's computer equipment and other electronic storage devices was not a general search and the executing officers did act as if the warrant's supporting documents imposed on the search limitations. United States v. Rosa, 626 F.3d 56, 66 (2d Cir. 2010).

[229] TEX. CODE CRIM. PROC. art. 38.23(b) (2017).

[230] *Id.*

[231] George E. Dix & John M. Schmolesky, 40 TEXAS PRACTICE: CRIMINAL PRACTICE AND PROCEDURE § 7:61, at 389 (3d ed. 2011).

[232] CRIM. PROC. art. 38.23(b).

[233] *Sims v. State*, 526 S.W.3d 638 (Tex. App.—Texarkana 2017, pet. granted).

[234] *Id*. at 640.

[235] *Id*.

[236] *Id*. at 641.

[237] *Id*.

Seemingly, Article 38.23(a) would require suppression of evidence obtained in violation of a statue: "No evidence obtained by an officer or other person in violation of any provisions of the Constitution or laws of the State of Texas, or of the Constitution or laws of the United States of America, shall be admitted in evidence against the accused on the trial of any criminal case."[238] However, the specific statutes in question "provide[] for civil actions, but no exclusion of evidence."[239] Reasoning that specific statutory language should control over general language, the court of appeals held even if the warrantless pinging was done in violation of the SCA or Article 18.21, the Exclusionary Rule is simply inapplicable apart from a constitutional violation.[240]

On discretionary review, Sims urges the court to apply the exclusionary rule or risk promoting the same tyranny the rule was designed to protect against.[241] In support, Sims argues that neither the SCA nor art. 18.21 prohibit suppression as a remedy.[242] Accordingly, the sweeping language of art. 38.23(a) should control as the Legistlature intended.[243] Regardless of its outcome, this case has major implications on the use of cell phone evidence.

E. Expert Qualifications and Opinions

Orin Kerr's criticism of *United States v. Wallace* demonstrates the need for properly limiting expert testimony. The expert should recognize the limitations of his or her opinion, and the Court should ensure the expert actually understands the data involved.

All lawyers should call on expert witnesses to testify about a cell phone's location when it is relevant to their case. Under Federal Rules of Evidence 702, a witness who is qualified as an expert by his skill, knowledge, training, or experience may testify at trial if: (1) the expert's knowledge will help a trier of fact understand the evidence or determine a fact in issue; (2) the testimony is based on sufficient data or facts; (3) the testimony was formed based on reliable principles and methods; and (4) the expert has reliably applied those principles and methods to the facts of the case.[244] Courts differ on whether an expert is needed to testify on information relating a cell phone's location and connection to a particular tower.[245]

Further, the Supreme Court has set forth four factors to determine whether a theory or technique is scientific knowledge that will assist a trier of fact in a given case.[246] These factors include: (1) whether the theory can be tested; (2) whether the theory has been subjected to peer review and publication; (3) a scientific technique's known or potential rate of error; and (4) if the theory is generally accepted.[247] These four factors have also been applied to theories or techniques used to identify information relating to the location of a cell phone during a time period in question.

In *United States v. Machado-Ezaro,* the defendant argued an expert's testimony regarding cell site analysis was not based on reliable methodology and should have been inadmissible.[248] The government countered that the FBI Special Agent intended to testify the cell phone was used by the defendant in a location near where a body was found, but was not stating the actual location of the user.[249] The government also offered evidence that the Special Agent's testimony would prove the phone must have been in a particular area to connect to a particular

---

[238] TEX. CODE CRIM. PROC. art. 38.23(a) (2017).

[239] Sims v. State, 526 S.W.3d 638, 642 (Tex. App.—Texarkana 2017, pet. granted).

[240] *Id*. at 642–43.

[241] *See* Brief of Petitioner-Appellant at 22–23, Sims v. State, No. PD-0941-17 (Tex. Crim. App. Apr. 3, 2018).

[242] *Id*. at 44–52.

[243] *Id*. at 27.

[244] FED. R. EVID. 702.

[245] *See* CONDES & AGUERO, *supra* note 32, at 29.

[246] Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 594 (1993).

[247] *Id.*

[248] United States v. Machado-Ezaro, 950 F. Supp. 2d. 49, 51 (D.D.C. 2013).

[249] *Id.*

sector and tower, but the Agent did not himself determine the cell towers to which a phone connected.[250] Still, the court found the proposed testimony admissible under *Daubert* because it was based on expert testimony that was grounded in scientific knowledge.[251]

F. Limiting Expert Opinion

In order to know how to offer or challenge testimony, you must first know whether you are dealing with data obtained from a cell phone service provider or data obtained directly from a cell phone itself. If the data's source is the cell phone service provider, it is helpful to assess whether the information is GPS or cell tower connection data. If the data's source is the device itself, determine whether the data is from GPS, WiFi, cell tower connection data, or location based services (a combination of the three stored internally).

Although expert witnesses may testify about a cell phone's location based on cell site tower connections, this testimony should be limited. In appropriate situations, GPS information showing a phone's proposed location may not be entirely accurate, and thus, can be challenged.[252] The GPS function on cell phones only works reliably outside where the handset has a clear view of GPS satellites; thus, GPS may not always produce accurate location results.[253] A 2013 study of several different smartphone devices concluded that, in open sky, ninety percent of all mapped positions fell within three meters of the baseline.[254] However, when placed under a canopy, there was significant interference with the mapping abilities.[255]

In *Brown v. State*, the court allowed a laywitness to testify about how GPS worked.[256] In *Brown*, a witness from a trucking company was permitted to share the GPS location of a truck because she "showed [it] was reliable . . . [and] established her understanding of the many systems the company used to track its drivers."[257] This should be the exception—not the rule.

G. Best Evidence Rule

In *United States v. Bennett*, Bennett's boat was searched by a joint task force targeting smuggling from Mexico to California.[258] A GPS found on Bennett's boat revealed Bennett traveled from Mexican waters to San Diego Bay. Testimony of his location based on GPS evidence was presented at trial.[259] The court held the testimony violated the best evidence rule because the GPS display the expert was referencing in his testimony only indicated he saw a graphical representation of the data from the GPS.[260] A print out of the GPS data would have been the best evidence, therefore, the testimony was inadmissible under the rule.[261] The conviction was ultimately reversed as this testimony was prejudicial to Bennett.[262]

---

[250] *Id.* at 55.

[251] *Id.* at 57.

[252] *See* CONDES AND AGUERO, *supra* note 32, at 41.

[253] *Id.*

[254] Jeff Shaner, *Smartphones, Tablets, and GPS Accuracy*, ARCGIS BLOG (July 15, 2013), https://www.esri.com/arcgis-blog/products/arcgis-online/field-mobility/smartphones-tablets-and-gps-accuracy/.

[255] *Id.*

[256] Brown v. State, 163 S.W.3d 818, 824 (Tex. App.—Dallas 2005, pet. ref'd).

[257] *Id.*

[258] United States. v. Bennett, 363 F.3d 947, 949 (9th Cir. 2004).

[259] *Id.* at 950.

[260] *Id.* at 953.

[261] *Id.* at 954.

[262] *Id.* at 955.

V. CONCLUSION: WHAT LIES AHEAD

As Chief Justice Roberts observed in *Riley*, "cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[263] Lawyers and judges must understand the significant privacy concerns involved as cell phone issues take their course through our legal system. To do that we must know the source of the data—either the cell provider or the phone itself—an increasingly important distinction after the decisions in *Riley* and *Carpenter*. Don't be the lawyer or judge who gets put on blast in the blogosphere.

Taken together, these cases show the general public's reinvigoration of a basic understanding of the purpose behind the Fourth Amendment: "to secure 'the privacies of life' against 'arbitrary power[,' and] 'to place obstacles in the way of a too permeating police surveillance.'"[264] Indeed, "Compelling comparisons are drawn between the infamous Lord Halifax's general warrants used in 1763 to seize all of a suspect's papers" and rummage unbridled for evidence of a crime—any crime.[265] Allowing the government a sneak-peak into our cell phones and cloud data with access to all of our files is exactly the type of invasion the Founders sought to prevent.[266] Worse, if the government obtains a citizen's data but never prosecutes, the citizen may never know the government has ever learned nearly everything about every aspect of his or her life, again similar to Lord Halifax refusing to return the papers generally seized for global inspection for evidence of a crime.[267]

Interestingly, this successful reinvigoration comes not from just the courts or citizens themselves but rather the companies trusted to keep citizens' personal and cloud data safe and secure. For example, "Apple assembled a team of 'legal luminaries' to successfully challenge the San Bernardino order," claiming it would lead to a "police state."[268] "[T]wo of the three most valuable companies in America have taken offensive against the federal government to assert the Fourth Amendment rights of everyone."[269] As a result of their success, many others are joining the fight.

The communal efforts have been successful, as evidenced by *Carpenter*. For a moment, it seems the Fourth Amendment stands for what its intended purpose. As lawyers, and members of the public, we have a duty to remember the reason behind the Fourth Amendment and apply it accordingly.

---

[263] Riley v. California, 134 S. Ct. 2473, 2484 (2014).

[264] Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (internal citations omitted) (quoting Boyd v. United States, 116 U.S. 616, 630, 6 S.Ct. 524, 29 L.Ed. 746 (1886); United States v. Di Re, 332 U.S. 581, 595, 68 S.Ct. 222, 92 L.Ed. 210 (1948)).

[265] Clark D. Cunningham, *Apple and the American Revolution: Remembering Why We Have the Fourth Amendment*, 126 YALE L.J. FORUM 216 (2016).

[266] *See id.*

[267] *Id.* at 226, 228.

[268] *Id.* at 216–17.

[269] *Id.* at 231; *see also* Microsoft Corp. v. United States (In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197, 200 (2d Cir. 2016).