CHAPTER 4

Mobile Phone Tracking

PHONE TRACKING

In the previous chapters, we covered how dangerous a phone can be, whether it be an old public switched telephone network (PSTN)-based phone or a new digital mobile phone. Although the chapter focuses on mobile phone attacks, it should be considered that just about every device with network connectivity these days can place you at the scene of the crime. It is also very disturbing that with mobile technology, devices are carried with you and not left in your home, placing you directly at the scene of the crime. That being said, your movements are being tracked and recorded and you should be aware.

When you are tracked with your mobile phone (or device), you are essentially giving your exact geographical position away to your telecommunications carrier. The radio towers that you use to obtain and maintain your signal are also used as reference to your exact position. Global positioning system (GPS) technology also aids in placing your location that we will discuss further in this chapter. Carriers can also track movement based on technology called location-based services (LBS). This technology can be used to assess specific coordinates as you use your mobile device. We will also discuss this technology further within this chapter.

In this chapter, we will also address how the US government is taking advantage of an outdated law on privacy and technology to track Americans. If you use your mobile phone, it will register its position with cell towers every few minutes, whether the phone is being used or not – and mobile carriers are retaining location data on their customers. As the government collects and uses this data, a record of your movements is being kept without your permission or knowledge.

Before we get into the specifics of how mobile devices are used for surveillance and reconnaissance, gathering information, tracking, and misuse, we must first understand the specifics of mobile technology and which types are most commonly used.

Mobile Phones

Since this book is about digital surveillance and reconnaissance and how to defend against attacks, we will not get too deep into the architecture of the devices themselves; however, we will cover the specific phone types and the specific attacks leveraged against them. It's important to know how they are used to track your movements and how they can be used against you.

Why is spying on mobile devices so important to understand? If you are a victim, let's look at what could be at risk:

- View SMS messages – Applications can record all SMS activities from the target phone. All sent and received messages can be recorded in an online account, even if the messages are deleted from the mobile phone.
- View call logs – Each call can also be logged by the application that will also be uploaded to your online account. This provides the caller and the time of call.
- Track GPS location – GPS tracking can provide your location at any time and be recorded to an online account.
- View photos and videos – All photos and videos taken can be recorded and sent to an online account.
- View contact list – A contact list of phone numbers can also be viewed and sent to an online account.
- Website URL logs – This can show that websites are visited and sent to an online account.
- Call recording – Your calls and messages can be recorded and retrieved and sent to an online account.

As you can see, with a simple application, your privacy is no longer secure and everything you say and do as well as where you go can be tracked.

Apple iPhone

Proprietary hardware, tightly controlled software, and a tightly controlled application store called iTunes makes up the Apple iPhone experience. This does not mean that you're safe from surveillance, far from it. It just means that it's less likely that malware will immediately infect your phone and allow you to be tracked.

As seen in Figure 4.1, the Apple iPhone is a handheld computer/phone that allows you to collaborate via applications, texts, e-mails, and phone conversations.

Tools and software (specifically Cydia) can be used to "crack" into the phone so that you can use it more freely; however, by doing so you open yourself up to more possibilities of being infected with malware. Regardless, many applications are available to load on the phone to track others beyond how they are already tracked via location services and tower acknowledgments.

FIGURE 4.1 Apple iPhone.

Any mobile device can be tracked in numerous ways; however, those that are more commonly used (such as the iPhone) have more applications developed for that specific purpose.

Google Android

Open Source driven, Linux-based Google Android phones are widely used next to Apple iPhones. Having multiple hardware vendors and a variety of operating system types, Android is extremely flexible. Google Play allows for application download and installation and many applications are available for tracking and reconnaissance of the phone.

As seen in Figure 4.2, the Android platform is highly customizable and if you are a professional at mobile phone development, many options exist to place a tracker on the phone without your knowledge. Also subject to malware attacks, the mobile devices produced can be easily tracked.

Android (as well as iPhone) allows for an attacker to download applications from their application stores to use for tracking such as Spying Droid that covertly allows an attacker to use one Android device as a camera unit and another Android device to view live audio and video from the first device. If conveniently placed, it could provide covert surveillance for information gathering. Another app that can be downloaded is called Couple Tracker, which allows an attacker to spy on another person such as a spouse for the purposes to get their location, see their messages, or to verify their location.

FIGURE 4.2 Google Android.

Just like iPhone, you may need a higher privilege level on your phone that may require you to root it or use super user access.

Windows Phone

Similar to Apple and Google, Microsoft has a mobile device called Windows Phone. The marketplace is where you can get applications for your mobile device and among them are the same spy applications that are available for all other major phones. It is susceptible to the exact same surveillance risks associated with Apple and Google devices.

As seen in Figure 4.3, Windows Phone is Microsoft's line of mobile phone devices. Recently, Microsoft acquired Nokia who is the primary maker of Windows Phone hardware and the merger has rebranded these companies as Microsoft Mobile.

Although it's a different company, it's the same exact set of risks, problems, and concerns associated around privacy.

Blackberry

An older mobile device type that has significantly evolved is the Blackberry from RIM Research in Motion (RIM). As seen in Figure 4.4, the Blackberry offers many of the same features as does Apple, Google, and Microsoft; however, the Blackberry has predominately been used in the business world of enterprise

FIGURE 4.3 Windows phone.

FIGURE 4.4 Blackberry phone.

companies and generally married to a Blackberry Enterprise Server that allows for advanced functionality. In the past few years, the Blackberry has undergone significant graphic user interface changes and enhancements in order to stay competitive with the other device offerings from Apple and others.

That being said, it too can be hacked and tracked just as easily as the others. Other devices exist and can be tracked as well. Following the same concepts as we covered, anything that works by providing an Internet protocol (IP) address, an assigned phone number, or an e-mail account can be easily tracked. Other device types and software packages allow for tracking ability. GPS devices, pads, and other mobile devices can be tracked. Microsoft's XBOX game console can not only be tracked but also can be viewed by an attacker inside your home through its sensor.

You should be concerned because what we just briefly covered is only half of the story. The other half is how the mobile devices you use give your location away without any application usage of any kind.

Phone Tracking

Phone tracking can be simply done by carrying your phone with you as you go about your day. So how is it done?

When a mobile device connects to a cell network, it registers with the carrier. When your mobile device is powered on, it emits a signal that is picked up by multiples towers. Your phone is triangulated by its distance from multiple towers. GPS receivers provide tracking information as well. Wireless signals can also be tracked in the same fashion. Shockingly, even if it is powered off, it may still be susceptible. In foreign countries, viruses (malware) have been distributed to keep the phone on enough to produce a signal for tracking.

As seen in Figure 4.5, when you carry your phone, it emits a signal that works with carrier cell towers and/or GPS satellites that provide you with the service, but also keep a log of your location within the system. This means that government agencies, law enforcement, or, if hacked, an attacker can also verify and validate your position at any time.

There are ways to also review these logs to trace your movements. So, if you travel from New York to New Jersey five days a week, your path to and from could be articulated from review logs at tower locations along that path. Of course, this is all deemed to be legal unless misused, but as we have learned, the government is collecting data to track the behaviors of suspected terrorists. They do this by collecting all data and then filtering on what they need. What seems to evade our private lives is that the information is in fact captured and available. It could be misused if an opportunity arose.

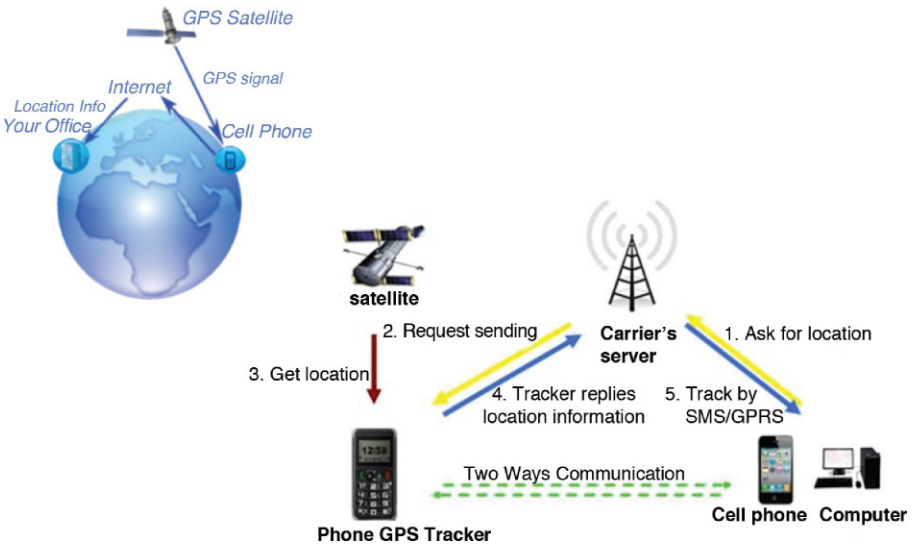

FIGURE 4.5 Example of phone tracking.

The Patriot Act

Immediately after the September 11 attack on the United States, the Congress passed the Patriot Act. The Patriot Act is an expansion of the surveillance laws allowing the government to spy on its citizens while reducing the oversight required to do so, fairly and with accountability. The bill was sent to vote without time for review, debate, or discussion and the threat of attacks was used to create a fear vote.

This act was created to expand surveillance laws by the government so that it had expanded record searching ability held by third parties (such as a telecom carrier), secret searches of private property without the need to inform the owner, and other expanded intelligence searches.

MALICIOUS TRACKING

As we can see, tracking can be done without your knowledge and at many different levels. Your mobile device although helpful and a needed fixture of your person, is now a mobile tracking device that can be used to find you, evade your privacy at any moment, or as a tracking tool for another malicious user, stalker, attacker, or threat.

Before we get into how to track a phone by example, it's important to understand the first steps to protecting yourself as much as possible. First, do not leave your phone unattended. Do not leave it unlocked. Do not leave it without a password. Use a strong password scheme. Make sure nobody is shoulder surfing you when you use your phone. In Chapter 8, mitigation strategies will

be covered in detail; however, it's important to note here that by practicing simple security steps, such as those just listed, you significantly lessen the attack surface.

Tracking for Reconnaissance

Not all phone tracking is bad. Many applications exist today to help you find a lost or a stolen mobile device. Other tracking applications are used to keep tabs on children you are responsible for. They can be (and often are) used for wrongdoing. As mentioned earlier, applications exist such as Google Play's Track Your Wife by Tryfon to track the activities of a possible cheating spouse. In the last section of this chapter, we will discuss how this type of action is handled legally but before we do, let's review why it's done and specifically how it's done. Technology has expanded our ability to keep tabs on others we distrust. In a relationship where someone is suspected of wrongdoing, applications exist to validate this malicious behavior to those willing to track it. Those who track it, usually the other party in the relationship, may be able to ascertain facts that they had first suspected but could not prove.

A tool that can be (and is commonly) used is one that does not appear on the phone itself, if hidden, is MSpy. This is a great tracking tool that once installed will basically give you all of the information about anyone's mobile device use. Although this tool can be used for good, such as tracking a child by phone, it can also be used to secretly spy on someone without their knowledge. Some of the features included with MSpy are:

- Dashboard tool – Overall dashboard used to get an overview of the tracked mobile device.
- Listen to incoming and outgoing calls – This will allow you not only see incoming and outgoing calls but also listen to them.
- Run SMS tracking – You can track all incoming and outgoing SMS text messages.
- Read e-mails – This tool allows you to see and read all e-mails associated with the target device.
- Perform GPS tracking of the target device – You can track the device via GPS and show locations via map.
- View photos and videos – You can view all digital media photos and videos on the target device.
- See calendar events and contacts – You can see all calendar-related information on the target device.
- Read chat and Instant Message (IM) conversations – Review all chat and IM conversations specifically via text.
- Track browsing history – You can see what websites are being used on the target device.

- View Skype messages – You can track all Skype data on the target device.
- Monitor WhatsApp messages – You can track all WhatsApp data on the target device.

You can also track Facebook data, Viber data, and much more. That being said, privacy is no longer an option to the unsuspecting user of the mobile device with a product such as MSpy configured on it. Again, it can also be used for good security reasons when you give a child a mobile device so that you can track usage as well as location. You can also restrict data being used on the target device with MSpy. However, when considering the surveillance that can be done especially without your knowledge, it could be worrisome to someone who does not know it is there.

As seen in Figure 4.6, we will begin to prepare an Apple iPhone for surveillance tracking. First, if you are attempting to track someone, you need to get access to the device itself. To do so, you can get access to the device in many ways. In this example, we will look at what many users are attempting to do as of the writing of this book – track a significant other or spouse. First, get the device and if password protected, you can either crack the password, of shoulder surf to get it. There are many ways to easily bypass the password of an Apple iPhone. Once you do, you need to jailbreak the phone. Jailbreaking a phone is done

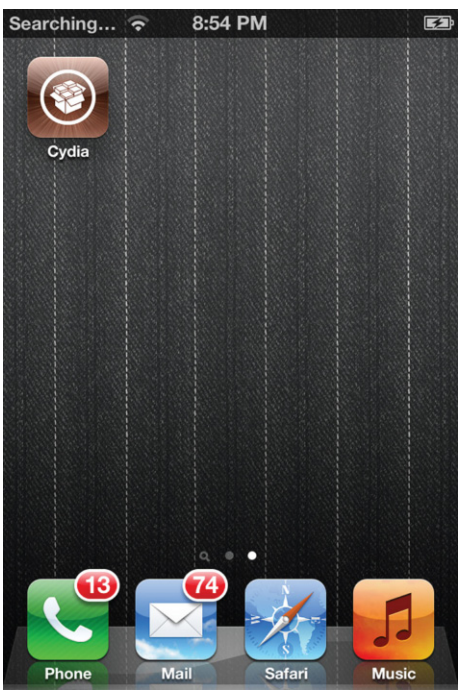

FIGURE 4.6 Jailbreaking and prepping a phone for tracking.

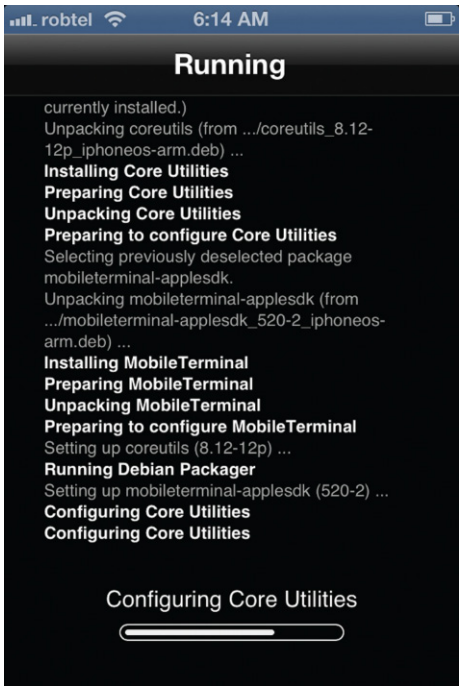

FIGURE 4.7 Installing and configuring MSpy.

quickly and easily, by downloading a package online that matches your iOS version, you can run the program, the phone will reboot and you will have full access to the phone.

Once Cydia is installed (part of Jailbreaking routine), you can open it and install and configure MSpy. You will have to purchase a subscription for their services and they can assist you with this process as well. Once you get a subscription and register the phone, you can configure the phone for tracking.

As seen in Figure 4.7, installing MSpy is quick and painless. You download the package and it installs on your phone and will drop an icon on the iPhone home page; however, it will be removed once the registration is completed.

Once MSpy is installed and you have registered the service, you can begin to customize the mobile device so that it can be tracked. As seen in Figure 4.8, you will need to turn on location services for MSpy in order to physically track the phone.

As seen in Figure 4.9, you can then hide the applications on the home page so whoever is using the device does not see the applications installed. This can be helpful so that once the victim uses the phone, they will not know that MSpy is installed on it. There is no visual existence so it can be hidden and kept secret.

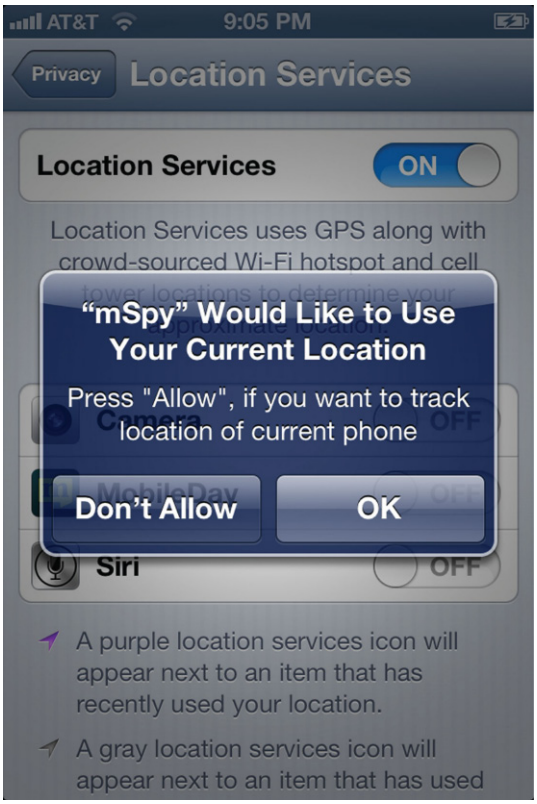

FIGURE 4.8 Turning on location services.

Once MSpy is installed, you can access the online dashboard to view all of the data and track the phone.

As seen in Figure 4.10, the dashboard can be used to view call logs (shown), text messages, listen to calls, track movement, and so on. As you can see, whoever is being tracked will not know and all interactions on the phone will be logged for viewing by the attacker.

It is possible that a very savvy user who knows how to go into the settings of their phone and nose around may stumble across the changes; however, it can be easily played off as an update from Apple as an example. It's rare that these changes are found unless the person who you are victimizing really know what to look for.

Lastly, for safety and possible furthering the attacks on the target phone, you should change the default password.

As seen in Figure 4.11, it is recommended that you change the default Apple password of Alpine as well as the default mobile password on your device. This

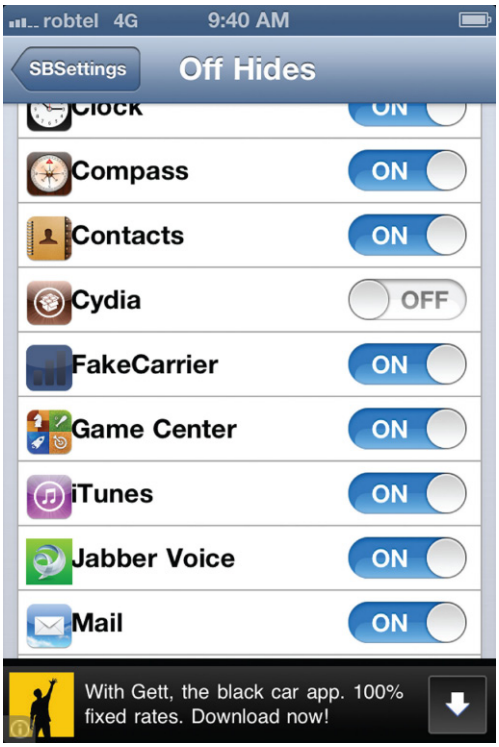

FIGURE 4.9 Hiding the applications on the system.

can be done, obviously, for security, but it can also be used to configure an Secure Shell (SSH) tool for remote access into the device from your personal computer.

You can of course use other tools such as StealthGenie and Mobile Spy instead of MSpy; however, MSpy provided the features needed for this example.

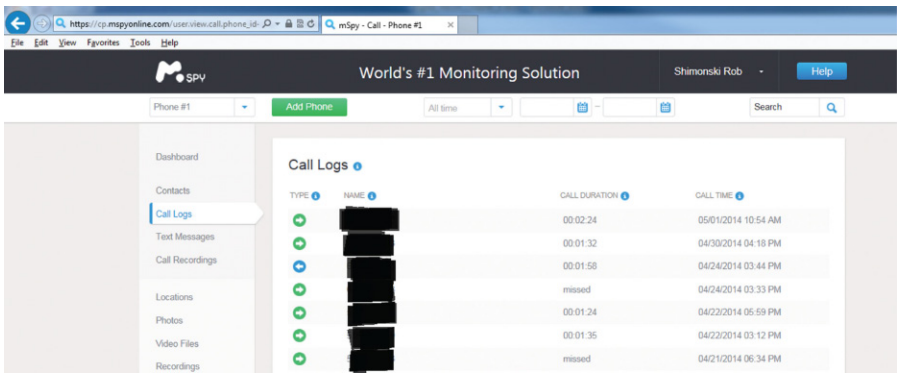

FIGURE 4.10 Using the MSpy dashboard.

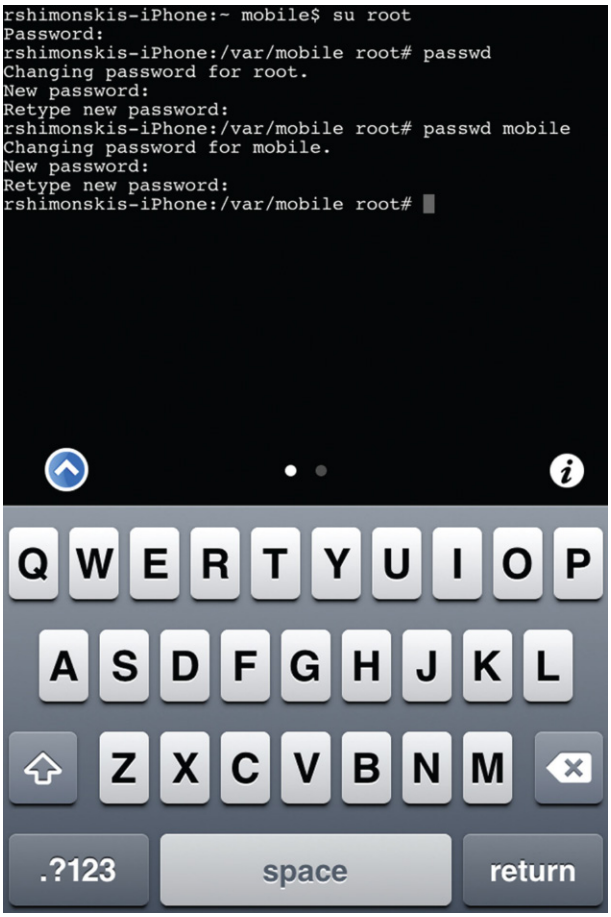

FIGURE 4.11 Changing the passwords on your mobile phone.

As well, although we configure this tool for use on an Apple iPhone, you can also configure this system on mobile devices from Microsoft, Google, and others; however, the services are the same and the outcome is similar, your privacy has been evaded.

Location-Based Services

Embedded within the mobile phones technology is a service called LBS. This allows location data to assist with providing enhanced functionality. The applications are developed so that you do not have to input information; the information required is simply queried from your device.

With Apple's iPhone, the operating system (iOS) is deployed with a standard LBS functionality that allows applications to be able to track where you are and

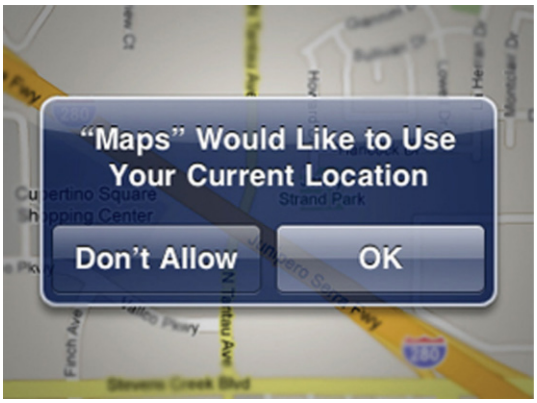

FIGURE 4.12 Using LBS.

report it to the querying application. For example, as seen in Figure 4.12, Maps can use LBS to track your current location on a map for the purpose of making your life easier.

This functionality, however, evades your privacy. When you use LBS, Apple is collecting real-time tracking location information on its user base. Privacy policies released by Apple have said that the data is collected anonymously; however, how do you know this to be factual? And even if it was collected anonymously, it could be reconstructed to identify individuals. Why would Apple need this information in the first place? When considering the amount of questions that come up about protecting privacy, it's easier to opt out and simply not allow any application to do your thinking for you.

Other legal concerns are raised about LBS. For example, with LBS enabled, someone who gains access to your mobile device could possibly use the device to trace back your steps through your social media accounts that also use this technology to "map" your traveling habits. As seen in Figure 4.13, other applications such as Google Maps also attempt to track your location through LBS.

It should be clear that your privacy is affected when you choose to allow software to track you; it should not come as a surprise that this data and the data

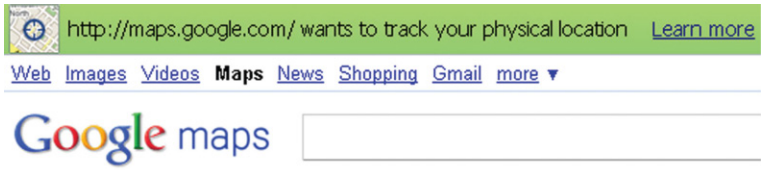

FIGURE 4.13 Google Map tracking.

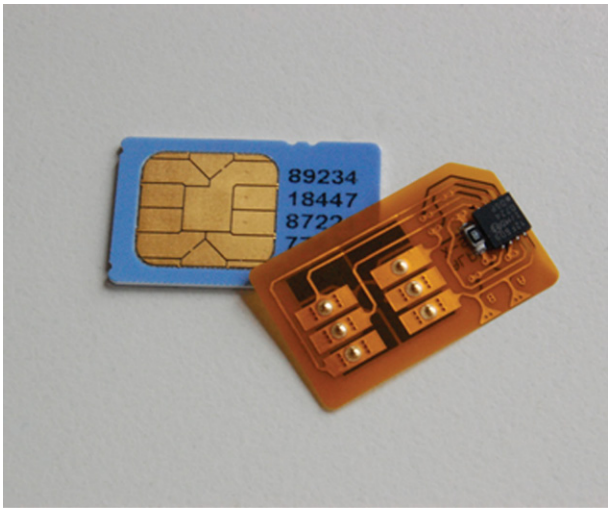

FIGURE 4.14 SIM chips.

stored on the servers that collect the data could be used to track you and gather information about your habits.

Tracking a SIM

Each mobile device used as a phone will have a subscriber identity module (SIM) card installed that uniquely identifies the device. The SIM card (or chip) will store information and allows the device to be tracked. The SIM will send out a signal to the carrier network in order to be used on the carrier network, but can also be misused. For good purposes, you can track your phone if stolen or lost. However, a phone can also be tracked maliciously through the SIM. As seen in Figure 4.14, SIM chips are commonly used in most if not all mobile phone devices.

To track a SIM easily, report your device stolen and contact your service provider or carrier. They may be able to track your device for you. You can also install GPS software (covered in the next section) to pinpoint the devices location via satellite. Apple uses a program called MobileMe that is a cloud-based solution to back up your phone; however, it can also be used to track your phone if lost. You can also install a SIM tracker application on a phone so that the movements of the phone can be tracked both in real time and historically.

Global Positioning System and Geolocation

A GPS is used to pinpoint the physical device location directly or through triangulation. As discussed earlier in this chapter, a GPS can use a satellite or a series of satellites to track movement of a device. For good purposes, GPS can provide you with mapping data for trips as well as to find a lost device. However, for

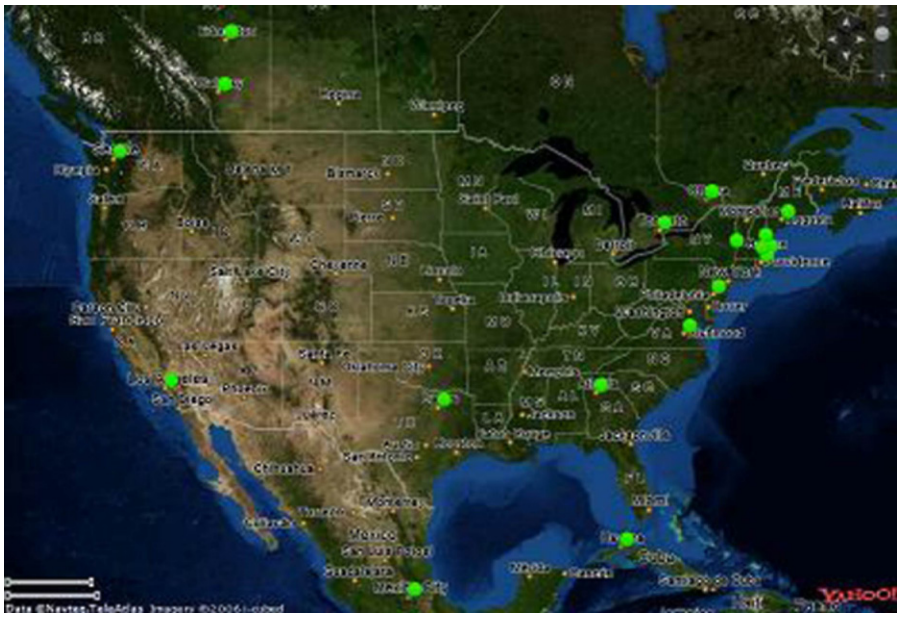

FIGURE 4.15 Yahoo Map tracking with latitude.

malicious purposes, GPS can show an attacker your exact position worldwide. Geolocation data can also be used to track device usage; however, it does so using information from other sources as well. TCP/IP can be used to assist with Geolocation. As seen in Figure 4.15, other applications such as Yahoo maps provide Geolocation data.

Google Mapping

Another major issue with the tracking of location by applications is the possible abuses that can take place with Google Latitude. In line with Geolocation tracking, Latitude can (with your permission of course) pinpoint your exact location on the Earth. Used in conjunction with Google Maps, Latitudes friend finder location-aware tool for your phone also combines with your Google Talk phone service.

As seen in Figure 4.16, Google Maps with latitude provide Geolocation data. Google LBS provide those with accounts the ability to track "friends"; however, if we were able to gain access to this data, we would be able to track victims without their knowledge.

What may seem worse is, Google has access to this data as well. Another concern would be, although privacy policies state that this data is not used in illicit ways, one can only guess what would happen if someone were to get their hands on this data for malicious purposes. The point here is it's still "collected."

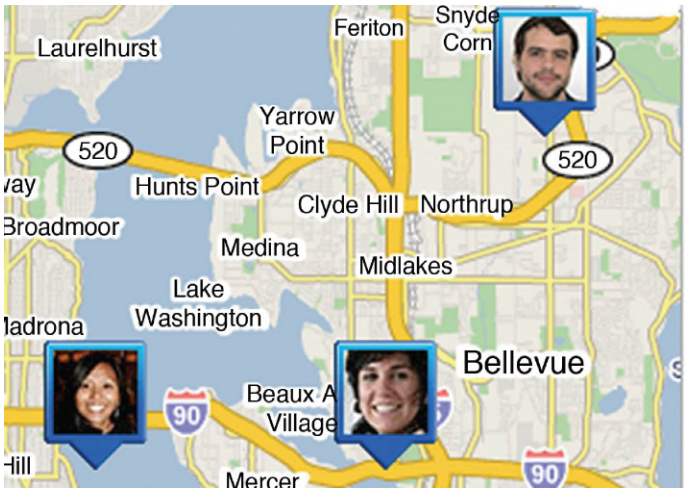

FIGURE 4.16 Google Map tracking.

Other tools that can be used on mobile devices are iLocalis, InstaMapper, and many, many more. As you can see, there is no shortage for phone tracking utilities in the market and if an attacker were to get their hands on the data they collect, it could be used for malicious purposes.

Google Glass Tracking?

As we move into the world of Google Glass and other wearable technology, one has to ask – how safe is this technology? How can it invade my privacy? The answer is simple – it is nearly identical to the mobile device you carry, except these are mobile devices you wear. As seen in Figure 4.17, Google Glass is a wearable mobile device that allows you to access the Internet and applications through a pair of glasses.

As technology develops and privacy and security risks are not addressed, more and more personal data will be collected and stored that can be used by those who may wish to track you. A large number of attacks can be launched aside from gathering of information through tracking. Man in the middle attacks can take place where an attacker can inject themselves between the source and the destination and pollute the conversations with false data. Eavesdropping attacks can take place where information is gathered and other attacks may be launched, for example, if bank account information is intercepted.

At a higher level, the governments we are supposed to trust with our security and safety are gathering data and analyzing it for patterns. Is it possible that someone could be falsely accused of a crime they didn't commit by simply being within the "pattern?" What about your ability to keep your life private? Where does privacy end and safety and security pick up? All of these questions

FIGURE 4.17 Google Glass.

need to be answered by those who are concerned about rights to privacy being stripped away; however, the digital age keeps us bound to the technological landscape in which we now live.

LEGAL AND ETHICAL CONCERNS

There are many legal and ethical concerns revolving around mobile phone tracking. For one, it is unethical to simply attempt to spy on another and evade their privacy either for malicious intent or otherwise. Marketing purposes in the opinions of many do not count … you should not be tracked.

The Location Privacy Protection Act of 2012 (S.1233) was introduced by Senator Al Franken (D-MN) in order to regulate the transmission and sharing of user location data in the USA. It is based on the individual's one-time consent to participate in these services (Opt In). The bill specifies the collecting entities, the collectable data, and its usage. The bill does not specify, however, the period of time that the data collecting entity can hold on to the user data (a limit of 24 h seems appropriate since most of the services use the data for immediate searches, communications, etc.), and the bill does not include location data stored locally on the device (the user should be able to delete the contents of the location data document periodically just as he would delete a log document). The bill that was approved last month by the Senate Judiciary Committee would also require mobile services to disclose the names of the advertising networks or other third parties with which they share consumers' locations.

In January 2009, a special report by the Department of Justice revealed that based on 2006 data, approximately 26,000 persons are victims of GPS stalking annually, including by cell phone. In December 2010, an investigation by the

Wall Street Journal revealed that of 101 top smartphone apps, 47 disclosed a user's location to third parties, typically without user consent. In April 2011, iPhone and Android devices were found to be sending Apple and Google location data, even when users were not using location apps and even though Apple users had no way to stop this. In June 2011, Nissan Leaf drivers discovered that their cars automatically transmitted their vehicles' location, speed, and destination to many third party websites accessed through the car's computer.

In September 2011, users of Windows Phone 7 smartphones discovered that their phones sent their location to Microsoft when the camera was on – even that app was denied permission to access location. Later that month, OnStar told its customers that it would continue to track their cars' speed and GPS locations "for any purpose, at any time" – even if those customers had ended their OnStar service plans. In November 2011, consumers learned that smartphones were sending location and other information to a firm called Carrier IQ – even though they had never heard of the company and had no way to stop this. In May and October 2012, the Federal Communications Commission (FCC) and Government Accountability Office (GAO) issued separate reports finding that mobile companies were giving their customers too little information about how their location information was used and disclosed to third parties. The GAO also found that industry self-regulation had been unclear and inconsistent. Unfortunately, most of these activities are entirely legal. Even after Jones, every time you use the Internet on your smartphone, companies are legally free to give or sell your location information to almost anyone they want – without your consent. While the Communications Act prohibits wireless companies offering phone service from freely disclosing their customers' whereabouts, an obscure section of the Electronic Communications Privacy Act of 1986 explicitly allows smartphone companies, app companies, and wireless companies offering Internet service to give their customers' location information to nongovernmental third parties – without their customers' permission.

The Location Privacy Protection Act of 2012 (S. 1223), sponsored by Senator Al Franken and cosponsored by Senators Richard Blumenthal, Chris Coons, Bernard Sanders, Richard Durbin, Robert Menendez, and Dianne Feinstein, will fix this outdated federal law to require companies to (1) get a customer's permission before collecting his or her location data or (2) sharing it with nongovernmental third parties. The bill will also (3) raise awareness and help investigations of GPS stalking and (4) criminalize the knowing and intentional operation of "stalking apps" to violate federal antistalking and DV laws. This bill does not concern or affect law enforcement location tracking, which is addressed in other legislation.

The bill was introduced with the support of a coalition of consumer privacy and antidomestic violence groups, including the Center for Democracy and Technology, Consumer Action, Consumers Union, the Minnesota Coalition for

Battered Women, the National Association of Consumer Advocates, the National Center for Victims of Crime, the National Consumers League, the National Network to End Domestic Violence, the National Women's Law Center, and the Online Trust Alliance.

Retrieved from:

http://www.franken.senate.gov/files/docs/LPPA_one_pager.pdf

and

http://thomas.loc.gov/cgi-bin/query/L?c112:./list/c112s.lst:1201

An interesting case of People versus Hall is a classic case on how tracking and mobile technology can be used in the court of law, the outcome, and the effect of using such technology. The defendant Alexander Hall was indicted for one count of murder in the second degree, four counts of assault in the first degree, and one count of criminal possession of a weapon in the second degree allegedly committed on October 12, 2005 outside a New York City Night Club.

Detective Rivera of the New York City Police Department conducted the investigation when one of the other defendant's disclosed his cell phone number. The cell records were then subpoenaed in hopes of being able to track the location the of the defendant's whereabouts to iron out the inconsistencies in each of their stories. T-Mobile's system automatically records the identity of the towers the second a call starts until it is disconnected that pinpoints exact locations. Information such as the cell customer's account information, name, date of birth, social security number, and call detail is already being retained for ordinary business purposes that were obtained by the People from T-Mobile Cellular.

Hall sought to suppress records obtained on the ground that such subpoena was issued without probable cause and in violation of Hall's constitutional rights. Hall also sought suppression of identification evidence obtained subsequent to the issuance of the subpoena. The evidence Hall wanted suppressed consisted of records relating to Hall's cellular telephone.

The people met their burden to establish their compliance with the Federal Stored Communications Act (SCA) (18 USC § 2703) that they contend provides authorization for the subpoena and the receipt of the subpoenaed information, but Hall argues they fell short of the constructional requirements for retrieval of cell site data and under this cases circumstances was used as a "tracking device." Under ECPA, cells are not considered tracking devices.

The court finds that the subpoenaed material was properly obtained.

There is no fourth amendment violation as the records obtained and the information gathered was property of T-Mobile and belongs to them for legitimate business purposes.

Hall's motion was denied.

People v Hall

People v Hall 2006 NY Slip Op 26427 [14 Misc 3d 245] October 17, 2006 Stone, J. Supreme Court, New York County Published by New York State Law Reporting Bureau pursuant to Judiciary Law § 431. As corrected through Wednesday, January 24, 2007

[*1] The People of the State of New York, Plaintiff,

v

Alexander Hall, Defendant.

Supreme Court, New York County, October 17, 2006

APPEA RANCES OF COUNSEL

Frederick Hafetz, Priya Chaudhry and Louis Freeman for defendant. Linda Ford for plaintiff.

OPINION OF THE COURT

Lewis Bart Stone, J.

On December 2, 2005, defendant Alexander Hall was indicted for one count of murder in the second degree (Penal Law § 125.25 [2]), four counts of assault in the first degree (Penal Law § 120.10 [3], [4]), and one count of criminal possession of a weapon in the second degree (Penal Law § 265.03 [2]), allegedly committed on October 12, 2005. Hall now seeks to suppress records obtained on November 4, 2005 by the District Attorney's office through a grand jury subpoena issued by the Honorable Michael Ambrecht, on the ground that such subpoena was issued without probable cause and in violation of Hall's constitutional rights, and also seeks to suppress identification evidence obtained subsequent to the issuance of the subpoena.

The evidence sought to be suppressed consists of records relating to Hall's cellular telephone (the cel) obtained by the People from T-Mobile Cellular, the carrier for the cel. At the hearing held on June 26, 2006, the People called three witnesses, Sue Johnson, custodian of records for T-Mobile, Police Detective Kevin Rivera of the 34th Precinct Detective Squad, and Assistant District Attorney Al Peterson of the New York County District Attorney's office. I find all such witnesses credible. The defense called no witnesses. After the evidentiary hearing, the court reviewed the written memoranda of law submitted by the parties and thereafter heard oral arguments. Findings of Fact.

On October 12, 2005, at approximately 4:11 a.m., outside of Club Viva located at 4168 Broadway, in Manhattan, three people were shot, one of whom, Tabitha Perez, was killed. The investigation conducted by detectives of the New

York City Police Department (NYPD) led to Hall and three of his friends, [*2] Sabin Abad, Christopher Ulanga, and Javier Gonzalez, all of whom had earlier been ejected from the club and had been involved in an altercation with the club's bouncers. Following the altercation, the four left in two separate vehicles, which had been parked in the adjacent parking garage. Shortly, thereafter, the People contend, Hall returned in one of the vehicles and shot and killed Tabitha Perez and wounded the other two victims.

Rivera, an NYPD detective, was assigned to investigate the case. An attendant from the parking garage provided Rivera with the license plate number of one of the vehicles allegedly used by one of the persons fleeing the altercation. The vehicle matching such plate number was a blue Acura, registered to Ulanga's grandfather. Ulanga was interviewed at the 34th Precinct on October 12, 2005 and he told Rivera that he was at the club with a friend named Mark, and that after they were there for a while he observed some type of dispute and thereafter left in the Acura with his friend Jay and went home. Ulanga disclosed his cell phone number to Rivera.

Following this interview, the People subpoenaed Ulanga's cell phone incoming/outgoing call records in order to identify Mark, Jay, or other people Ulanga was in contact with that night as possible witnesses or suspects. After receiving the records of calls from Ulanga's cell phone, the People then subpoenaed subscriber information for the phone numbers that Ulanga's phone had made or received around the time of the shooting and the hours immediately following. This investigation led to cell phones belonging to Hall, Gonzalez, and Abad, each of whom were subsequently interviewed.

Gonzalez, who was interviewed by Rivera on October 23, 2005, stated that on the evening in question, he was at the club with Abad, Ulanga, and Hall, and was involved in the altercation and that afterward he drove to the Bronx and dropped off Abad.

Abad, who was interviewed by Rivera on October 25, 2005, stated that he was in the club with Gonzalez, Ulanga, and Hall that evening and he was escorted out when he tried to light a cigarette inside the club and that during the dispute outside the club he was injured on the head, and then drove to the Bronx with Gonzalez.

Hall, in the presence of counsel, was interviewed by Rivera on October 28, 2005, at which time he stated that he was at the club with Ulanga, Abad, and Gonzalez, and stated that during the dispute he grabbed Abad and told him "don't worry about it, we will see him later." Hall claimed that after the dispute, the four went to the garage to retrieve their vehicles and all four went directly to the vicinity of Hall's apartment on West 96th Street. Gonzalez stayed and slept on the couch and Ulanga and Abad left. Hall stated that he was not in the vicinity of the club at the time of the shooting.[*3]

Following the Hall interview and recognizing the conflict between the stories of the four as to where each was at the relevant times, the People obtained a court order for cell site records for each of the four cell phone numbers, to enable them to determine the general location of where calls were made from the cell telephones of each of the four men between the time the four left the club and the time of the shooting. T-Mobile's system automatically records the identity of the antenna tower to which a particular cell phone was connected at the beginning and end of each call made or received by that phone.

Based on the affidavit of an assistant district attorney attesting to the facts gleaned in the investigation, Honorable Michael Ambrecht, sitting as the grand jury judge, issued subpoenas to T-Mobile for such cell site information for the cell phones of the four suspects (including the cel), between October 10 and October 13, 2005. T-Mobile, which had recorded such information in the ordinary course of its business and retained such records for its own business purposes, complied, providing subscriber information for the cel showing Hall's account number, name, address, social security number, date of birth, and home telephone number and call detail records from October 10 to October 13, 2005, the dates requested in the subpoena. These records show the start time, end time, and duration of each call made or answered by the cel for the specified dates as well as cell tower records identifying which T-Mobile cell tower received the signal from the cel at the beginning and end of each call, thus, identifying the approximate location of the cel when completed calls to or from it were begun and ended that evening and identifying the telephone number of the caller or recipient of the call. These records provide no information by which the location of the cel may be ascertained other than in connection with completed actual calls made or received. It is this cell site information that Hall seeks to suppress.

Cellular telephone or "wireless" networks, operated by T-Mobile,[1] are divided into geographic coverage areas, or "cells." Each T-Mobile cell contains an antenna tower that sends a signal to cellular phones on the T-Mobile network through which such telephones may transmit and receive calls while located in such coverage area. The size of a particular T-Mobile cell is determined by a number of factors, including, but not limited to, the radio reception range, the topography of the surrounding land, the presence of buildings, and prevailing weather patterns, and the expected cellular [*4]telephone traffic in the area. T-Mobile cell size ranges from several hundred feet[2] in some urban locations, such as portions of Manhattan, to more than 15 miles in suburban and rural areas.

---

[1] The testimony was specific to T-Mobile's operations and records. As this case relates solely to the Hall's motion to suppress the specific T-Mobile records obtained, this court does not find on the basis of this hearing that all cell phone carriers systems operate in a similar manner as to lead to the same result had the records of a different carrier been in question.

[2] A city block between numbered streets in Manhattan is, for example, traditionally about 200 feet.

Generally, each T-Mobile antenna tower provides 360 degrees of coverage. As a T-Mobile cell phone and its user move from place to place during a call, the system automatically switches the connection to the T-Mobile cell antenna tower that provides the best reception. For this process to function correctly, each cell phone using the T-Mobile network must periodically transmit a unique identification code to register its presence within each T-Mobile cell. T-Mobile then uses this unique number, together with information identifying the antenna tower to which the cell phone is currently connected, and in many cases, the 120-degree portion or "sector" of the tower facing the cell phone, to route calls to and from the cell phone. Each T-Mobile cell tower is assigned a unique number that is automatically used to route calls and that is recorded in the case of completed calls to indicate the starting and ending cell involved in such call.

Although T-Mobile cellular phones turned on by the user regularly emit signals that are received by the nearest tower, even when no call is being made, unless the subscriber makes a completed call or a completed call is made to such subscriber, T-Mobile's system does not automatically make or keep any records of such signals or which cell site received such signals and did not, in the case of the cel, make or keep any such records where calls were not made or recorded during the period relevant to this case.

The T-Mobile system has the capacity, however, to allow "pinging" of a T-Mobile telephone that has been turned on by its subscriber, even if the subscriber is not making a call, to determine the cell in which such phone is located at the time of the "ping." To do so, T-Mobile would have to expressly act to cause its network to do so, but cannot reconstruct such information for periods to when such action was taken. The subpoena neither called upon T-Mobile to "ping" the cel nor is there any evidence that T-Mobile "pinged" the cel to generate the records, or information in question here. Thus, the information which Hall seeks to suppress did not arise from "pinging."

The People contend that they have met their burden to establish their compliance with the federal Stored Communications Act (SCA) (18 USC § 2703) which they contend provides authorization for the subpoena and the receipt of the subpoenaed information. Hall does not dispute that the People have established [*5]compliance with the SCA, which requires "specific and articulable facts showing that there are reasonable grounds to believe that the … records or other information sought[ ] are relevant and material to an ongoing investigation" (18 USC § 2703 [d]), but argues instead both that such statutory standard falls short of constitutional requirements for the retrieval of cel site data, and further that the cel under the circumstances of this case was a "tracking device," and that, as a result, the People have not met their obligations under a different federal statute, the Electronic Communications Privacy Act of 1986 (ECPA) (18 USC § 3117 [b]). Under ECPA, the People must seek prior

court approval based on probable cause, before they may use a "tracking device." As a third contention, Hall claims that by obtaining the cell site records, the People invaded the privacy of Hall's home, as "warrantless monitoring of an electronic tracking device in a private residence which is not open to visual inspection, violates the Fourth Amendment."

Central to Hall's second and third contentions is that the cel is a "tracking device." The People do not contend that they have complied with ECPA, but instead assert that the cel is not a "tracking device" under ECPA and, as a result, compliance with ECPA's higher standard was unnecessary. As to the claim that obtaining cell site records represented a warrantless monitoring of an electronic tracking device in a private residence, the People counter both that the cel was not a tracking device, and that there was no "monitoring in a private residence."

As the parties' positions as to Hall's second and third contentions turn mainly on whether the cel was a "tracking device," it is necessary to address such contentions. Hall's claim under ECPA must be analyzed under the definition of a tracking device in ECPA. Hall's Fourth Amendment claim, however, being constitutional, cannot rest alone on such statutory definition of tracking device, as Congress in enacting ECPA may have, as a discretionary matter, balanced privacy interests of individuals against law enforcement's interest in a way more favorable to privacy concerns than those mandated by the Constitution. Similarly, if, as the People contend, the monitoring of broadcasts to and from cellular phones recorded outside of a person's home is a matter of federal statutory concern, rather than a constitutional principle (as will be discussed below), Congress may, in its definition of a tracking device in ECPA, set a balance that would have been short of the constitutional balance in favor of privacy mandated by the Fourth Amendment with respect to tracking devices placed in a suspect's home.

Under ECPA, a tracking device is an electronic device that permits the tracking of a person or thing. Case law has expanded the definition to include devices that fit the definition, although they were not originally designed or intended to track movement. The ECPA is designed to prevent police authorities from tracking movement through such a device without obtaining prior court approval based on a [*6]probable cause standard. The record here does not establish that the cel was designed or intended to be a tracking device but was designed to be a cellular telephone to be used on the T-Mobile network that retained and recorded information within its system, in the regular course of business for billing purposes, which information was disclosed pursuant to the subpoena.

It is also clear that the cel could be transformed into a portion of a device to track the cell in which the cel was located but only if the T-Mobile network was directed to "ping" the cel, so long as the cel was on, and that no such direction

or pinging took place. However, the record is also clear that in the T-Mobile network, only the nearest cell tower would register the presence of the pinged cell,[3] thus determining the location of the cell only within an area the size of such cell, and could not determine the direction or speed of the person carrying the cel unless and until that person finished the call in another cell.

To determine what is a tracking device for the purpose of ECPA, it is necessary to look to the purpose of ECPA, its legislative history, cases, and the ordinary meaning of words. The ECPA was enacted in 1986, which although only 20 years ago, represents an almost antediluvian age with respect to present technology and communications systems. The United States Senate report accompanying adoption of the ECPA, in its glossary of terms, defined an "electronic tracking device" as a one-way radio communication device that emits a signal on a specific radio frequency. This signal can be received by special tracking equipment and allows the user to trace the geographical location of the transponder. Such "homing" devices are used by law enforcement personnel to keep track of the physical whereabouts of the sending unit, which might be placed in an automobile, on a person, or in some other item.[4]

This almost quaint definition essentially defined the classic "bug" that the police would surreptitiously attach to a car or a person's clothing to enable them to be followed in real time. It is not surprising that the courts, faced with a more generic statutory definition, were able to extend the concept to two-way devices such as cellular telephones which the police now often use to perform the same function as a [*7]"bug" placed by them.

Such federal courts routinely require a showing of probable cause under the ECPA as a condition of allowing the police to use cellular telephones as tracking devices on a prospective basis, that is, to gain future information relating to a suspect's movements. These cases do not address certain differences between the cellular telephone and the classic bug, that is the fact that in most cases, the phone subscriber, being aware of his possession of the phone, would not necessarily take it with him at all times and might turn it off for short or extended periods. The courts seem instead to assume that a cell phone owner will keep his telephone on and with him as a general matter, thus making a cellular telephone rigged to show the functional location equivalent of a bug. Because technology has changed the state of the art far from the classic bug, the courts are not of the same mind as to how to interpret ECPA and the results vary

---

[3] While there was testimony that during some periods of high cellular telephone usage, a call may be routed through an adjacent tower, rather than through the nearest, Johnson's testimony made it clear that the times the relevant calls were made in the middle of the night were not periods of high use, and accordingly only the nearest tower would be recorded as handling actual calls.

[4] S Rep No. 541, 99th Cong, 2d Sess (1986).

among courts. The consensus seems to be that prospective tracking through a suspect's cellular telephone requires a finding of probable cause under ECPA.

In re Application for Pen Register and Trap/Trace Device with Cell Site Location Auth. (396 F Supp 2d 747 [SD Tex 2005] [hereafter cited as Texas I]), cited by both parties here in support of their positions, the court described the tracking device in such case as follows: "Tracking devices have progressed a long way. Most agencies now have sophisticated tracking devices that use cell site towers or satellites … These types of tracking devices are usually monitored from the law enforcement agency's office. Through the use of computers, a signal is sent to the tracking device (it is pinged), and the tracking device responds. The signal is picked up using cellular telephone cell sites or satellites. The location of the tracker, and therefore the vehicle, is determined through triangulation and a computer monitor at the agency office shows the location of the vehicle on a map. These tracking devices are very accurate, and can differentiate between a vehicle traveling on an interstate highway or the feeder (service) road. The tracking devices will also provide the direction of travel and the speed the vehicle is traveling." (Id. at 754.)

Using the technology described above, the cellular telephone in question together with the computer, cell sites, and satellites and the use of triangulation, the location of the cellular telephone can be tracked in real time. There is no question that the combination of these factors made the operation addressed by the court in Texas I one involving a tracking device.

The record here shows the cel to fall far from this level of convergence with the "bug" problem that ECPA addressed. The record here shows that the T-Mobile [*8]system would only, upon "pinging," determine the single cell tower nearest to the cel, thus precluding any possibility of triangulation that is the basis for all GPSs and the court's decision in Texas I. Even assuming the factual conclusion that a governmental agency had the capacity, using its own computers through the T-Mobile network, to monitor the location of the cel in real time, the facts established at this hearing show that T-Mobile could not, at the time in question, actually have done so and there has been no preservation of data to permit even such a capable governmental agency of now tracking Hall's movements as so described in Texas I. As the Texas I court said (at 751), "By a process of triangulation from various cell towers, law enforcement is able to track the movements of the target phone, and hence locate a suspect using the phone." Here, such scenario did not create the information that Hall seeks to suppress.[5]

---

[5] While it is clear that federal government agencies have the capacity to triangulate from "pinging" cell phones, carriers are not required to have such a capacity. (See United States Telecom Assn. v Federal Communications Commn., 227 F3d 450 [DC Cir 2000] [discussing that the New York City Police Department request to the Federal Communications Commission (FCC) to require cellular telephone carriers to have the ability to triangulate was rejected].)

In expanding the concept of a tracking device from the original transponder "bug" to cases where cellular telephones are involved to reflect changes in technology, the courts have determined that, where the cell phone, satellites, or cell antennas, and the carrier's system and computers located at law enforcement offices to "ping," triangulate, and analyze data work together to create the functional equivalent of a bug, the parts may each be treated as a "tracking device."[6]

The information in question arose from the ordinary use and operation of the cel, and not its putative possible secondary function of a tracking device had the government pinged and triangulated (which it would not have done on the evening of the alleged crime as the police had not ascertained the phone number of the cel until many days later). Thus, for the purposes of ECPA, the cel was not a tracking device.

With respect to the Fourth Amendment concerns as to the "intrusion" into Hall's [*9]home, the question is easier. For the same reasons set forth above, the cel could not, on the evening in question, be analogized to a bug, thus differentiating the cel from cases where the People may have bugged a defendant's home. As there was no triangulation, the subpoenaed records can no more than show that Hall was, at certain times when he used the cel, in the vicinity of his home, and cannot even show whether he was inside or outside of his home at the time of any call. On the other hand, had Hall used a landline from his home, his telephone records would have more accurately shown his whereabouts at home[7] and such records could have clearly been obtained by subpoena without the showing of a probable cause. This argument is at best a makeweight, and is hereby rejected. The Constitutional Standard of the Stored Communications Act.

Hall concedes that the People have met the standard that the SCA provides for a subpoena thereunder, but asserts that, as to the cell tower information which Hall seeks to suppress, the SCA is constitutionally insufficient under the Fourth Amendment standards. The US Constitution Fourth Amendment, adopted in the eighteenth century, when there were neither telephones, cellular telephones, nor an understanding of electronics,[8] provides: "The right of

---

[6] Some courts also require the government to provide the cellular telephone to bring such a system under the ECPA. (See In re Application of United States for Order for Disclosure of Telecommunications Records & Authorizing Use of Pen Register & Trap & Trace, 405 F Supp 2d 435 [SD NY 2005].) Such case, which Hall claims was wrongfully decided, is the only reported federal case in the district in which this court sits. If such case controls, Hall's contentions would fail as Hall provided his own cellular telephone. It is therefore not surprising that Hall asserts this case to be wrongfully decided. This court need not determine the correctness of such case as the issue there involved prospective data collection and not historical data from which triangulation site information could not be ascertained, as is the case here.

[7] Perhaps, if he used a portable telephone, he might even have been outside of his home.

[8] Benjamin Franklin may have had some understanding of electricity.

the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or thing to be seized."

While additions to the judicial gloss on this amendment are constant, certain aspects seem to have evolved over time as they relate to this case. An initial inquiry is whether the papers (and an attendant information) in question are the property of the person seeking to protect them (including those papers, which another holds for them) under circumstances where there is a reasonable expectation of privacy or whether such papers or information belong to someone else.

It is well settled, for example, that a defendant has no legitimate expectation of privacy and no cognizable Fourth Amendment interest in bank records and, therefore, lacks standing to challenge a subpoena for them. (United States v White, 401 US 745 [1971]; see United States v Miller, 425 US 435 [1976]; Matter of Cappetta, 42 NY2d 1066 [1977]; Matter of Shapiro v Chase Manhattan Bank, N.A., 53 AD2d 542 [1976]; Cunningham[*10]& Kaming v Nadjari, 53 AD2d 520 [1976]; Matter of Democratic County Comm. of Bronx County v Nadjari, 52 AD2d 70 [1976].)

The same principle has been applied to the records of a telephone company relating to a person's account. (See Smith v Maryland, 442 US 735 [1979]; People v Di Raffaele, 55 NY2d 234 [1982].) On a parallel track, the electronic emanations from telephones, intercepted or tapped or overheard outside of a person's house, have not received constitutional protection under the Fourth Amendment. As the Fourth Amendment in the nineteenth century could never have contemplated the interception of electronic waves, where there was no intrusion into a house, it was left to the Congress to address the new technology. The Congress did, by adopting a series of laws to regulate privacy issues in the electronic and telecommunications areas, and continues to readdress this issue from time to time as technology changes. Central to this regulatory scheme have been the Federal Communications Act enacted in 1934, the ECPA enacted in 1986, the Communications Assistance for Law Enforcement Act of 1994, which strictly regulated the disclosure of the content of electronic communications, and the SCA, enacted in 2006. The Congress is at present holding hearings on pretexting and related matters such as the use of data brokers that may lead to further legislation in this area. Hall cites a press report of issues raised at these hearings.

Over the period where Congress has regularly legislated in this area, balancing disclosure and access issues, and expressly providing for stronger privacy rights than in the Fourth Amendment standards under the FCC, rights equal

to the Fourth Amendment standards in the ECPA and weaker than the Fourth Amendment standards in the SCA, Congress has acted with the assumption that the Fourth Amendment is irrelevant because of the nature of electronics and telephones, relegating the appropriate determination of balancing to the Congress to do so by statute, under its powers to regulate interstate commerce.

To support his broad constitutional challenge to the long-standing statutory scheme and understanding of the Congress in areas where it has been regularly revisiting issues and legislation, Hall cites a recent Indiana District Court case. (In re United States, 2006 WL 187684, 2006 US Dist LEXIS 45643 [ND Ind 2006].)[9]

In such case, the federal District Court for the Northern District of Indiana upheld a decision of a magistrate, as not being clearly erroneous. The magistrate found that the People had sought both prospective and historical data. The court, [*11]after reviewing the federal statutes, concluded that a request under the SCA combined with a request under the pen register statute (which authorized a real-time future recording) could not bypass the probable cause requirement. Although there was broad language, the case does not expressly address what historic information may be obtained without showing of probable cause under the SCA in the absence of a pen register and trap-and-trace device having triangulation capacity.

Thus, this court finds that there is no Fourth Amendment infirmity to the SCA. The Fourth Amendment does not apply to disclosures thereunder because the information, having been gathered by T-Mobile for its own legitimate business purposes, belongs to T-Mobile, not Hall, and because the Fourth Amendment does not apply to the interception of electromagnetic waves outside of a person's home, so as to constitute the acquisition of such information as a search or seizure. As Hall concedes that the People have followed the standards in the SCA for the subpoena, Hall's objection to such information is rejected.

As this court finds that the subpoenaed material was properly obtained, no analysis is necessary regarding the subsequent identification evidence nor is it necessary to determine whether there was an independent source to provide the basis for Hall's arrest.

Hall's motion is denied.

Retrieved from:

http://law.justia.com/cases/new-york/other-courts/2006/2006-26427.html

---

[9] Otherwise, Hall concedes, as the People have urged, that the federal cases address subpoenas for prospective information and do not address constitutional questions of the quantum of support required for a subpoena for historical data, the issue here.

SUMMARY

As we have learned, tracking is done quite simply because of our wanting (and needing) to carry a mobile device with us everywhere we go. We can be mapped, tracked, followed, and stalked with ease because of our devices. In this chapter, we discussed how to track movement and activity through a user's mobile phone. All major mobile platforms were covered to include iPhone and Windows Phone devices. We looked at apps that can be used to track our movements on a dashboard.

The government is taking advantage of outdated laws on privacy and technology to track Americans like never before. As long as it is turned on, your mobile phone registers its position with cell towers every few minutes, whether the phone is being used or not, and mobile carriers are retaining location data on their customers. We discussed how you can take care to ensure that you limit how you are tracked.

Page left intentionally blank