Cell Phone Investigations™: Narcotics Operations

Cell Phone investigations™: Narcotics Operations was specifically designed for personnel tasked with utilizing cell phone data in narcotic investigations. This course derives much of its substance from the longer national course Cell Phone Investigations™ by Aaron Edens. Topics within include: Searching for phone numbers, determining the provider, locating the legal or subpoena compliance department and specialize investigative techniques including: cell phone tracking and dropped phones.

Aaron Edens
Police Technical

Table of Contents

Welcome!

Good morning and thank you for attending this **POLICE TECHNICAL** course.

My name is Thomas M. Manson, founder of **POLICE TECHNICAL**, the company which is presenting this technical training course. Today you will be an attendee in a course which **POLICE TECHNICAL** and your instructor have been preparing for many months, and, truthfully, have been preparing for many years.

POLICE TECHNICAL has worked for several months to make your class today a reality. Each year we receive training requests from agencies across the country, and every successful class is the culmination of 4-6 months of coordination, marketing, and logistics. A May or June class likely began with a training request from the previous year.

Your instructor has also worked for many years preparing to teach this class. In addition to several years of law enforcement experience, many dedicated to the subject of your class; he or she has completed a lengthy process with **POLICE TECHNICAL** to become one of our instructors. This process involves a documented hiring process, a thorough background investigation, a detailed instructor and materials development process, and a continuing program of mentorship.

POLICE TECHNICAL and our instructors work hard to provide superior quality training for law enforcement in computer applications, online investigations, and forensics. I can tell you without hesitation, "Your course today will be one of the best you have ever had in this subject, and your instructor is one of the best in the field of law enforcement".

I know you'll find this class valuable, but if ever want to talk with me about your experience, or if you would like to talk about bringing a **POLICE TECHNICAL** training course to your agency or department I would happily speak with you.

Enjoy your class, and thank you again for attending this **POLICE TECHNICAL** course.

Respectfully,

Thomas M. Manson
POLICE TECHNICAL
812-232-4200 | www.policetechnical.com | info@policetechnical.com

Our History

In 2004 **POLICE TECHNICAL LLC** was establish to further professionalize the law enforcement training process created by Thomas M. Manson.

In 2007 **POLICE TECHNICAL** was recognized as a Sole Source Provider by federal law enforcement agencies, offering a level of training unavailable from any other source. **POLICE TECHNICAL** incorporated in 2009 to provide a suitable structure to expand business operations.

In 2010, **POLICE TECHNICAL** scheduled more than 50 national training courses (primarily PowerPoint® for Public Safety™).

In 2012, 6 new courses were being taught by instructors.

Searching for Phone Numbers

Instead of just checking a phone number in Google, try these other resources.

Pipl

Pipl is a free internet search engine that not only automatically checks Google, but also searches what is known as the 'deep web'. Pipl initially was limited to a search for name and phone number but has expanded to include email addresses, user names, and business names. I have found the results to be surprisingly good.

Metasearch Engines

Another method is to use a metasearch engine. A metasearch engine is simply a web service which queries multiple search engines at the same time and consolidates the results on one page. Using these free services it is possible to search Google, Yahoo, Bing, Ask.com, and About.com all at the same time. Dogpile.com, mama.com, and metacrawler.com are all good metasearch engines.

Commercial Database Services and Companies

Most law enforcement agencies have access to a commercial database service such as Accurint or CP CLEAR. These companies aggregate data from a wide variety of commercial and government sources to form as complete a picture as possible of an individual or business. Where exactly do these companies obtain their information? They won't tell you. Some company representatives, usually salespeople, will allude to having exclusive access to various super secret squirrel data sets. In reality, most of the information comes from three primary sources:

Public/open source government records and databases such as court filings relating to bankruptcies and judgments, real estate assessor records, and, in some states, driver license and criminal records

Publicly available information such as data from social networking sites, blogs, and forums

Non-public information from commercial sources such as financial institutions and utilities. This information can also include so-called credit header information consisting of dates of birth, social security numbers, and addresses. Credit header information is data obtained from credit reporting agencies but which does not include the corresponding financial information.

While these databases are good, no single database aggregator is going to be able to acquire data from every source. These databases also have another inherent issue which can be a double edged sword. As a commercial database aggregator compiles data from their sources, the compile them and can automatically create a relationship between entities, addresses, and people. For example, a cellular phone subscriber cancels his service with a particular provider in order to change to another service. The subscriber's phone number is eventually recycled and issued to another customer, in this case a female. During that time the first customer's financial institutions continued to report the phone number to the credit reporting agencies, as he had yet to change his phone number with them. Some commercial databases would now associate both subscribers with the same phone number and could even infer there was a relationship between the two when, in fact, they have never met. This is particularly true with several of the prepaid cellular service providers who can recycle their phone numbers in as little as four to six weeks.

Commercial databases can be a tremendous advantage during criminal investigations, but they are not without their drawbacks. They should not be viewed a definitive, nor should they ever be the sole source of information.

LP Police

Most law enforcement executives are familiar with the bigger names in the commercial database industry. However, there are other smaller companies which do just as good a job as the larger companies or who have specialized data sets which the larger companies lack. An often overlooked database aggregator is LP Police. Their cellular telephone number database is very good for certain providers and it is relatively inexpensive compared to some of the other companies. However, I have found some of their other data sources to be very dated when compared to identical results from other databases such as Choicepoint or Lexis Nexis.

iTACT

Another excellent database is iTACT provided by TargusInfo. This company has a very comprehensive dataset from a variety of sources, including at least some financial services companies, including some major banks. Targus allows for batch importing of target numbers and batch downloading of the results which is very helpful when dealing with a large number of inquiries. Furthermore, the service automatically provides information regarding the provider and whether the phone number has been ported to another provider (more on both of these topics later). Unfortunately, the service is more expensive than many of the other providers and reportedly they will only allow Federal law enforcement subscribers. The good news is the service is subscribed to by most High Intensity Drug Trafficking Areas (HIDTAs) who can perform the checks at your request for free.

A Free Alternative

Among the many commercial database services arrives a newcomer; TLO XP. What makes TLO XP different? The service provides the same results, or very similar results, as the other major database services. What sets the company apart is that it provides their services free to law enforcement…forever. What's the catch? I haven't found one yet. The search results are comparable to any of the other paid services and they have developed some advanced features which are not found with the other companies' products. I was able to run approximately 200 side-by-side searches with TLO XP

and another major commercial database. The results were almost identical. In 12 cases TLO XP had better, more current information than the other service. In two instances the other database had better results than TLO XP.

The cost savings for most law enforcement agencies can be significant and it is possible to equip every officer in a department with access instead of just a few key individuals. TLO XP can be reached at 888-493-2209 or CustomerSupport@TLO.com

Determining the Provider

Once you've completed your basic records checks and internet searches and made the decision to get a court order or search warrant for the records associated with the phone number, you need to determine who to serve with your legal process. Many investigators use a free internet service found at www.fonefinder.net. This website allows an investigator to minimally enter the first seven digits of a telephone number and get an immediate response as to the geographic location of the phone number and who the likely telecommunications provider is. I applaud the dedication and hard work of the web site developer who administers fonefinder.net. But for law enforcement investigations the service falls short in several areas, and because of this, I do not recommend it be used.

Here is a quick and dirty laundry list of problems that I have encountered with fonefinder.net:

1. *Fonfinder.net does not, and can not, take into account number portability.* Number portability, commonly called 'porting', refers to a customer retaining their phone number but changing from the provider who initiated service with the number to an entirely different provider. Porting is immensely popular as it allows consumers to shop for lower priced service while keeping the same phone number. However, fonfinder.net does not track these changes. From fonefinder.net's FAQ page: "Due to act of Congress, any telephone number in the USA can be "ported" away from its geographic nexus and default telco ownership, to a new telco. After a port, a new

telco is assigned to the specific number. FoneFinder cannot track these numbers' telco because the official owner of the porting database is Neustar which has a nondisclosure agreement which prohibits anyone from releasing porting information. I wish I could provide this information to you, but am prevented from doing so. Bottom Line: FoneFinder is inaccurate to the extent that numbers have been ported." Serving a court order, search warrant, or subpoena to a provider of a ported number can delay your investigation by several weeks or months. Number portability and determining the appropriate provider will be addressed later in this section, but for now it you should know that fonefinder.net does not and cannot track any changes in the provider and should not be used.

2. *Fonefinder.net may give you incorrect company information.* Fonefinder.net lists the name of the communications company when the phone number was initially assigned but this does not necessarily reflect the legal entity name which the subpoena compliance department of the provider will require. Addressing your legal process to the wrong company name can cause them to reject your request and delay your investigation.

3. *Fonefinder.net does not track the sale or transfer of phone transfers between companies.* It not uncommon for phone companies to sell, trade, or transfer blocks of phone numbers which have been assigned to them to another company. For example, in the jurisdiction where I work a large telecommunications company owned most of the prefixes for landline phone numbers. As landline phones were progressively abandoned the company was left with a large number of phone numbers without subscribers. At the same time, a prepaid provider experienced significant growth in the area and negotiated a deal with the larger company to purchase the unused phone numbers. If you run those phone numbers today, fonefinder.net will still show the number as being serviced by the larger company and not the prepaid provider.

In lieu of using the service of www.fonefinder.net, I recommend the website www.numberingplans.com. The data is the same but numberingplans.com also offers several tools for decoding the unique serial numbers on mobile devices such as the IMEI and IMSI (more on what these numbers are and what they mean later.)

Obtaining Current Provider and Contact Information

There are several methods for obtaining the current provider and contact information for a given service provider. One of them involves using the free services of a telecommunications group to help you. Did you ever wonder who decided area code 213 would cover Los Angeles and area code 415 would cover San Francisco? The North American Numbering Plan Administration (NANPA) assigns area codes and prefixes to geographic regions. It is also the clearinghouse for number portability through a subsidiary organization known as the Number Portability Administration Center (NPAC). NPAC has several services available for law enforcement agencies and public safety answering points (PSAPs). NPAC allows registered users access to a system called Interactive Voice Response (IVR). User of IVR call a phone number (no I'm not going to list it here), enter a personal identification number, and then the target phone number. An automated recording then notifies the user if the number was ported or not. If the number was ported the IVR system will indicate who the new provider is. If the number was not ported the IVR system will simply state the number has not been ported and other methods to check who the provider is will need to be used. More information on IVR can be found at http://www.npac.com/lawenforcement/faq.shtml

Another quick and easy way to determine who the current provider is to a cellular phone number is www.wirelessamberalerts.org. The purpose of the site is to allow consumers to register to receive Amber Alerts via text message. Once you enter a phone number, the site lists the cellular provider or directs you to the provider's home page. This website also factors in number portability as it is linked directly into the NPAC database. This service does not work for landline numbers and will not provide you with any information on where to serve your court order or search warrant.

All of the techniques described above are useful for determining who the cellular service provider is at the time of the request. However, you may run into significant challenges if you are trying to ascertain who the provider was on a phone number from two years ago. None of the services listed have provisions for determining historical provider information.

You must determine the provider who serviced the phone *during the time period for which you are seeking the records* and the IVR system from NPAC will only tell you if the number was ported and who the current provider is. If you are investigating a phone number from a year old case you should remember to check for whether the number was ported anytime during that time frame. There is a fee based service which is provides not only historical provider information but a number of other services as well. The Telephone Company Subpoena Generator (TCSG) from Telco Solutions

maintains a database of all telecommunications providers in the United States and includes the subpoena compliance contact information for those companies. An especially helpful feature of TCSG is that it will provide the 24 hour emergency contact information, if available, for the provider which can save precious moments in a critical investigation. Using their service it is possible to enter a date range and identify all of the providers who serviced that particular number during that period of time. For example if you are interested in an entire year of call detail records for a target phone number, TCSG will identify which carriers serviced the phone number and provide the contact information in the event the subscriber changed providers during that year. As the name implies, TCSG will also automatically generate a court order or search warrant for the investigating officers jurisdiction and import all of the relevant content such as the investigators contact information, the service provider's subpoena compliance contact information, the target phone number, and the dates requested. TCSG can also batch process numbers so all of the targeted telephone numbers are sorted by provider. For example, if you input 100 phone numbers, TCSG will combine the phone numbers by provider so all of the phone numbers which go to AT&T are on one form, all of the phone numbers for Verizon are on another, etc. This feature is an incredible time saver for the investigator who would otherwise have to manually lookup and batch all of the targeted phone numbers together. Also, it makes presentation to a judge much simpler as he or she only has to sign a few documents and not all 100. TCSG offers a free 30 day trial which I encourage you to use.

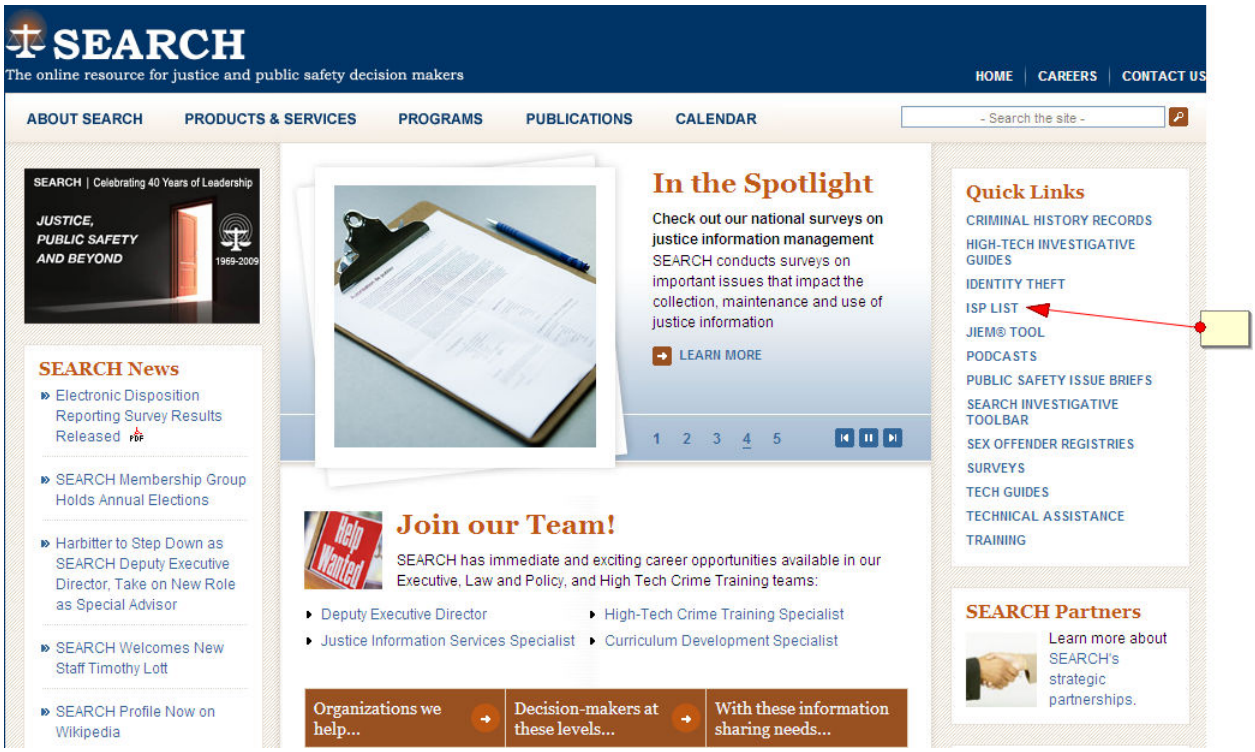
Neustar, the company that administers the IVR system for NPAC is reportedly going to offer a suite of products for their advanced Local Number Portability Enhanced Analytical Platform (which they call LEAP). Currently the major difference appears to be a web interface and the ability to batch import 100 phone numbers at a time. Batch importing is an important feature when dealing with a large group of target phone numbers such as those resulting from pen register and wiretap investigations. Another key feature of the LEAP system is the identification of alternate service providers. Some phone companies will market and service their accounts but the actual phone transmissions are handled by another provider. In order to obtain records from these types of providers it is necessary to submit a court order or search warrant to one company for the subscriber information (name, method of payment, etc.) and another court order or search warrant to the company which actually handles the phone calls to get the call detail records. LEAP's forthcoming features will also include a historical ported number research feature which will allow an investigator to

research which company has serviced a particular phone number as far back as 2005. There is also some indication LEAP will allow for subpoena generation and possibly electronic submission to the servicing phone companies. Automated submission of legal process to communications companies would be a tremendous time saver fo r both the investigating agency and the receiving company. Until those features are fully implemented it may make sense to use the services of TCSG instead. LEAP indicates their annual subscription fee, which is based on the amount of phone numbers submitted, will range between $500-5,000 annually. The higher end fees, which would only be applicable if an agency was submitting tens of thousands of numbers, are several times higher than TCSG's.

Location the Legal or Subpoena Compliance Department

Almost every major cellular service provider has a dedicated subpoena compliance department housed under the umbrella of their legal department. Smaller regional carriers, prepaid calling card providers, and some voice over internet providers (VOIP) may not have any formalized process for receiving legal process from law enforcement agencies. I participated in one investigation involving a calling card company where the entire staff of the company consisted of two people and they had no idea how to respond to a legal demand for records. It is important to weigh the investigative value of the records sought from smaller companies versus the potential for compromising your investigation by intentional or inadvertent leaks.

SEARCH, The National Consortium for Justice Information and Statistics, is a nonprofit membership organization which provides high technology investigative training, including cellular phone forensics training, among other services. At their website, www.search.org, they maintain an Internet Service Provider (ISP) list of legal and subpoena compliance contact information, including many cellular service providers. The information is supplied by and updated by other investigators so it is typically very current.



Metro PCS

Online Service:	MetroPCS
Online Service Address:	2250 Lakeside Blvd. Richardson, TX 75082
Phone Number:	800-571-1265
Fax Number:	972-860-2635
E-mail Address:	subpoenas@metropcs.com
Note(s):	It may take anywhere from 1 to 3 days for subpoena or court order requests. For general questions email: leaquestions@metropcs.com
Last Updated:	August, 2010

Another method is to simply check the name of the provider and 'subpoena compliance' in your favorite search engine. This typically works with larger providers but may not work with smaller companies.

Finding the Phone: An Alternative to Traditional Cell Phone Tracking Techniques

For a long time, may in the law enforcement community were convinced the cellular service providers were not providing all of the information or assistance they could. The belief wasn't that the phone companies were deliberately doing so, but that the subpoena compliance people were not aware of the technological capabilities of the underlying system. It shouldn't have been surprising that the employees of the legal department didn't have the technical expertise or even the means to extract additional information which could be relevant for law enforcement investigations. Unfortunately, they are usually the first, and often times the only points of contact for most law enforcement officers.

Eventually, information began to leak out. There were 'hidden' capabilities for recovering information from cell sites. It wasn't that the cellular companies were deliberately keeping the information to themselves. Rather, law enforcement officers were not asking the write questions and they were speaking to the wrong people.

One of the areas of information which has been recently 'discovered' is known as Per Call Measurement Data. PCMD is an exciting feature built into the equipment of some of the largest cellular service providers and has been sitting under the collective noses of law enforcement, and many subpoena compliance departments, for years.

Per Call Measurement Data (PCMD)

PCMD was originally referred to as Measurement Data in Call Records (MDCR). Both MDCR and PCMD are engineering terms referring to techniques used to measure the effectiveness of cellular service in a particular area. PCMD collects select measurement data on every completed call including information regarding the nature of terminated, dropped, and normal calls. Another data set collected by PCMD is the time it takes a signal to leave a cellular handset and the return back to the tower. It is this information which can provide previously unavailable information regarding the location of a particular handset.

PCMD was originally designed to be used for quality assurance purposes by gauging the number of dropped calls in a particular area. Based on this information a cell site engineer could recommend re-orienting a cell tower or other changes to improve the coverage in a particular area. However, someone within Alcatel-Lucent, one of the major manufacturers of cell tower equipment, discovered PCMD is accurate enough to be used for location based marketing without any upgrades to the existing cellular infrastructure or the customer's equipment. Because the speed of a cellular signal is a known constant it is possible to calculate the distance the handset is from the tower by measuring the time it takes for the signal to make a roundtrip. When combined with the cell sector information, there is now an opportunity to gauge how far away the handset is from the cell tower. This might not seem like an immediately revolutionary data set. Knowing that someone is three quarters of a mile away from a cell tower in the middle of downtown Atlanta is not likely to produce any great leads for missing persons or fugitive tracking. However, the data can be much more accurate than it initially appears.

Unlike the cell site and sector information obtained from call detail records, PCMD is captured not only for every phone call, but also for every text message and data event. Traditionally, most call detail records do not capture the cell site or sector used during text messages or data events such as voicemail and email notifications. These are not phone calls so the cellular service providers have no motivation to capture the information. PCMD is captured anytime there is a connection or data event between the cell site and the mobile device.

PCMD data has both quality assurance and location based marketing information applications and is already built into the existing cellular infrastructure. Subsequently, PCMD is able to provide relatively accurate location based

information. Is it accurate as GPS? No way. But it does add a dimension when combined with other information such as the cell site and sector. PCMD is not going to magically locate someone's handset but it is going to provide investigators clues which they might not otherwise have.

Now for the bad news. PCMD is only found in Alcatel-Lucent cell site products on code division multiple access (CDMA) networks. CDMA coverage in the United States is approximately 50% of the market but not all CDMA providers use Alcatel-Lucent equipment. Currently, PCMD is made available to law enforcement pursuant to proper legal request or exigent circumstances on the Sprint-Nextel and Verizon Networks only. In theory, it should be available from any cellular service provider using Alcatel-Lucent equipment on a CDMA network. Unfortunately, only those two providers acknowledge the information is available and are able to extract it for law enforcement use.

Here's some more bad news. PCMD is extremely perishable information. It appears the data may only be available for 7-14 days. This is not something that is going to be routinely preserved with the receipt of a preservation letter pursuant to 18 USC 2703(f). If your suspect or victim is using one of the two providers who acknowledge their ability to collect and retrieve PCMD, you must request the information as quickly as possible. I have seen PCMD data which was much older than 14 days but it was extremely sporadic and would not be useful in most criminal investigations.

Another limitation of PCMD which falls into the bad news category is that it is not real time information. The data is collected at the switch level and then updated to a call file hourly. Again, this is not done in real time so there will be a delay between when the information is captured and recorded and when it available for review.

PCMD records a tremendous amount of information. It does not come to you nicely formatted and with a cheat sheet for easy interpretation. Because there is no documentation it can be very easy to become confused by PCMD data. You may need to get the assistance of a cell site engineer or an electronic surveillance specialist in order to make sense of it. Fortunately, Verizon translates this information for you during exigent circumstances requests and will be able to tell you the distance, measured in meters, between the handset and the cell tower.

Verizon

PCMD is routinely provided to law enforcement officials pursuant to exigent circumstances requests, such as in missing persons cases, by Verizon. They refer to it as Real Time Data (RTD). However, they do not provide RTD/PCMD during routine requests, such as court orders and search warrants. This may be due to the fact that exigent circumstances requests are handled through the electronic surveillance division of Verizon, the people who provision wiretaps and pen registers, and not through the subpoena compliance department. You must specifically ask for RTD/PCMD in your court orders, subpoenas, and search warrants or you will not receive it.

Sprint

Sprint offers its L-Site service to law enforcement officers. This allows an investigator to activate the GPS positioning feature of a targeted device on demand. Consequently, many investigators forget about the availability of PCMD data from Sprint. As with Verizon, if you do not specifically request PCMD from Sprint, you will not receive the information.

Specialized Investigative Techniques

Cell Phone Tracking/Cell Site Emulators AKA "Triggerfish"

"Triggerfish" is the formerly classified code name for equipment used for tracking an individual cellular device. The equipment works by emulating a cellular tower and querying the particular serial number of a given device and measuring the signal strength to the device. This allows the operators to locate the device and, hopefully, the user of the device. Due to the cost of the equipment, "Triggerfsh" equipment is usually maintained by Federal law enforcement agencies (FBI, Secret Service, etc.), state law enforcement agencies, and large municipal law enforcement agencies.

In order to be used effectively, "Triggerfish" relies on an operational pen register in order to locate the cell tower and sector most recently used by the device. The "Triggerfish" team will then go to the area covered by the cell sector and attempt to locate the device. In my experience, the equipment is extremely accurate but relies on skilled technicians operating the device, a responsive and competent surveillance element, some degree of intelligence regarding the suspect's associates, and last but certainly not least, an active cell phone associated with your target.

If your agency requires the use of the equipment, I suggest checking with a larger state investigative agency. Federal law enforcement will use their equipment to assist local law enforcement investigations however; they typically require 'adoption' of the case. This can sometimes be a long and cumbersome process depending on which federal law enforcement agency you approach. Many times they are required to replicate the investigative work already completed in order to ensure a federal standard is met.

"Triggerfish" is often used synonymously with "Stingray" which is a companion product using the same technology for different purposes. "Stingray" emulates a cell tower and queries all devices within it's limited range. The function of "Stingray" is to attempt to isolate a suspect's previously unknown cellular device.

Dropped Phones

It is not uncommon for criminals to change their phones and/or phone numbers frequently. Sometimes this is done because of law enforcement surveillance (real or suspected), non-payment of their bills, law enforcement confiscation of the device, or the fact that criminals frequently lose their phones (sometimes to other criminals). However, many criminals don't actually abandon the device or throw it away. This is especially true with higher end phones which may

contain a large amount of content the criminal wants to keep possession of such as pictures, videos, music, games, or other applications.

The most frequent method of 'dropping' a phone is to simply change the number. Make sure to check with the provider to see if they have not simply changed the phone number.

If they do discard the device or lose it through other means, many criminals will stay with the same service provider and simply report the handset as lost or stolen and re-establish service using the same subscriber information.

Some criminals believe that by changing the Subscriber Identity Module (SIM) card on the phone they have defeated law enforcement's ability to track them. However, the International Mobile Equipment Identifier (IMEI) of the phone handset remains the same. Using a court order or search warrant, check with the provider to see if the IMEI is still active with a different SIM card.

Calls to Destination Searches

Cellular service providers can also do what is known as a "calls to destination search." This is a specialized computer search of their records for everyone else who has called your target phone number during a given time frame. This may be especially helpful a suspect has his caller ID blocked or called a phone number where the caller ID is not displayed or captured.

Here's how a calls to destination search works. Let's assume your agency receives a threatening phone call on the main business line. The caller specifically threatens to assassinate a particular officer in a specialized unit. Many criminals know that calls to 911 or the non-emergency line are automatically traced, even if they have caller ID blocking on their number. In this case, the suspect presumably knew this and called the business phone number for the department in order to make his threats. The caller ID of the suspect was not displayed or captured during the call, even when he was transferred to the dispatch center. Based on the specificity of the threat the department believes a credible threat exists against the officer. Traditional investigative methods would likely involve researching the officer's previous arrests and significant incidents in an attempt to identify likely suspects. However, in this instance the officer is assigned to a specialized enforcement unit targeting street gang members so the suspect list is long and distinguished.

In this case it appears impossible to attempt to identify the phone number of the suspect. However, this is not the case. The first step in attempting a calls to destination search involves identifying the specific time frame when the call was received. Even a small law enforcement agency receives a large number of phone calls on their main business line so narrowing down the time frame is essential. Narrowing down the time frame can be a double edged sword. Too narrow and you may miss the incoming call. Too broad and you may include multiple results which will all need to be researched. In this instance the approximate time the call was received is identified and an additional minute is added to be on the safe side. The next step is to identify all of the communications service providers, both cellular and landline, who cover your area. In a large metropolitan area this can be an intimidating appearing number of companies. However, the effort is worth it in this case-particularly if you are the officer who received the threats. Once you have identified all of the companies you will send them all a signed Court Order directing them to perform the calls to destination search. In essence, the Court Order directs them to search their entire call record database for any of their subscribers who called the particular phone number, in this case the main business number for the police department, during the specified time frame. For example:

Conduct a calls-to-destination search for the period 1/1/2012 1400 PST to 1/1/2012 1405 PST, of Urban PSC call detail records (CDRs) (date, time, duration, originating number, destination number) to identify any and all Urban PCS_mobile telephone numbers used to place calls to the following numbers: 510-555-7272.

Be sure to include additional language directing the provider to provide the subscriber information and call detail records for any subscriber they identify as making a phone call to the target number.

Calls to destination searches can be done anytime the date, time, and receiving phone number are known but the calling phone number is not known. Other uses for calls to destination searches can include:

A large scale drug dealer will not give an informant his phone number and only makes outgoing calls to the informant from a caller ID blocked phone number.

Fugitive investigations in which a family member or friend acknowledges receiving a phone call from the suspect but are unable or unwilling to provide the suspect's phone number.

Calls to homicide tip lines wherein the caller's information is so specific they must have firsthand knowledge of the crime.

Caller ID Spoofing

Caller ID spoofing is the use of technology to cause a telephone network to display a number on a receiving phone's caller identification (caller ID) system which is not in fact the true originating phone number.

There are a variety of technological methods for spoofing caller ID but the advent of voice over internet protocol (VOIP) systems have made spoofing easy and inexpensive. The most common method for spoofing caller ID is to use a subscription based service or a web based interface. Anyone can purchase a number of prepaid spoof minutes from a variety of internet based providers. These minutes are similar to a calling card and the purchaser is assigned a PIN number and an access number. The user then contacts the access number from any landline or mobile phone, enters their PIN number, enters the phone number to be called, followed by the phone number they want displayed. Some services offer additional features such as voice alteration and recordings of the calls emailed to the user at the conclusion of the call.

Caller ID spoofing has been used by criminals in a variety of harassing and stalking type crimes. Several high profile instances involving caller ID spoofing involved making 911 calls to report false crimes in order to elicit a high profile response from law enforcement. The action has been coined 'SWATing'. According to published report numerous instances of SWATing have resulted in tactical units responding to reports of violent crimes only to find unsuspecting subjects who have been victimized by this 'prank'.

In order to understand how caller ID spoofing works, you must understand what is transmitted when you make an outgoing phone call. When you make an outgoing phone call a packet of data is transmitted which contains the following data fields:

ANI (Automatic Number Identification)-ANI is the phone number you called from

ANI II (Automatic Number Identifier II)-ANI II is a two digit code containing information about the type of phone number you called from such as landline, coin operated payphone, correctional institution, mobile phone, etc.

CPN (Calling Party Number, also sometimes referred to as CID-Caller ID, CLID-Calling Line Identification, and/or CNID-Calling Number ID)-This is also the phone number you are calling from. However, the data in this field is able to be manipulated unlike the ANI.

CPN data is designed to be manipulated for a number of legitimate reasons. For example, CPN data contains a marker which designates if the calling number is private or can be displayed. If the number is flagged as private, the system displays 'PRIVATE' in lieu of the number. CPN data is also changed on outgoing phone numbers originating from a private branch exchange (PBX) used by a private office or organization. Many law enforcement organizations use a PBX which displays a general outgoing phone number and not the desk number of the originating officer or investigator.

Caller ID spoofing takes advantage of the ability of CPN information to be manipulated and changed. Using voice over internet protocol (VOIP) technology, caller ID spoofing providers can change the CPN data to display the data entered by their customer.

Costs for these services vary depending on the total number of minutes, also called credits, purchased. One popular internet vendor offers plans consisting of anywhere from 25 credits for $4.95 to 2,500 credits for $299.95. A credit is equal to one minute of talk time and five credits for a spoofed text message. Payment is as easy as entering your credit card number or using PayPal.

Some law enforcement agencies have explored using caller ID spoofing in their investigations with mixed results. There are a number of drawbacks for using caller ID spoofing during law enforcement investigations. Some agencies have reported running out of minutes or credits in the middle of a call which caused them some obvious difficulties. The other challenge involves returned calls. If the spoofed call is unanswered, attempts to return the call to the spoofed number may reveal that the phone call did not actually originate from that number.

The Truth in Caller ID Act of 2009

In December 2010 the President signed the Truth in Caller ID Act. The Act makes it a federal crime "…to cause any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value…" This law is a watered down version of other legislation which would have essentially stopped caller ID spoofing. Violators of this law face the possibility of fines for every instance they misuse caller ID. There is an exception in the law for law enforcement officers conducting "any authorized activity." Unfortunately, many of the caller ID spoofing countries are based overseas and are not covered by this law.

Caller ID Spoofing Weaknesses

Caller ID spoofing suffers from a couple of weaknesses which can be exploited during law enforcement investigations. Since commercial caller ID spoofing services first started, the number of companies have dwindled and consolidated into a few large providers. These companies faced the possibility of prohibitive regulation in the Truth in Caller ID Act of 2009 and seek to avoid any further legal restrictions which may force them out of business. This may cause some of the larger companies to cooperate with law enforcement legal process requests. In fact, in some of the 'SWATing' stories discussed earlier, it appears those companies did cooperate with law enforcement investigations. However, somewhat complicating the issue is the fact that some of these companies are based in Canada. This would likely involve seeking assistance from the FBI Legal Attache for assistance in service of process.

Users of the VOIP service Skype have the ability to change the displayed number on caller ID systems. Cases involving Skype are notoriously difficult to investigate due to a variety of reasons including the fact they are based in the tiny country of Luxembourg. Skype does respond to law enforcement requests but they do not always capture information which may be relevant to an investigation. Skype does generate user logs on the host computer which can show calling activity using the service. If a suspect in a caller ID spoofing case is known or believed to be using Skype, a forensic examination of their computer may reveal evidence contained in the activity log which can assist in prosecution.

Another vulnerability of caller ID spoofing is that it is not feasible, at this time, to alter the ANI. As discussed earlier caller ID spoofing changes the CPN but the underlying ANI remains unchanged. This is one reason why calls to 911 public safety answering points (PSAPs) still reveal the incoming call, even when the caller ID blocking in enabled.

The ANI is also accessed when calls are made to toll free phone numbers such as 800 numbers. As the owner of the toll free line is paying for the phone call, they are entitled to see the underlying phone number.

The ability of toll free numbers to reveal the ANI is the basis for the service known as Trap Call. Trap call is a service offered by one of the major caller ID spoofing companies. Trap Call offers users a subscription service which allows the user to reject unknown or caller ID blocked incoming calls. Those rejected calls are then routed to Trap Call's service which is, in essence, an enhanced toll free number. The call is then routed back to the subscriber's phone which can be answered or sent to voicemail. Trap Call then sends the subscriber a text message which contains the ANI of the incoming call. Trap Call also offers a premium service which offers the subscriber the added feature of running the incoming phone number through public records databases for subscriber information, digitally recording and transcribing incoming conversations, and creating black lists of prohibited incoming callers.

Trap Call does not work with all cellular service providers. According to their website, Trap Call only works with AT&T, T-Mobile, Verizon, and Sprint. Many of the prepaid providers such as Metro PCS and Boost are not supported. Trap Call also has applications which can be installed on phones using Blackberry, Apple, and Android operating systems.

I learned about Trap Call first hand during a wiretap investigation. The case agent in the investigation had the main suspect under surveillance. In order to confirm the suspect was still using the phone number which was the target of the pending wiretap, the case agent made a phone call to the suspect using his department issued phone. The suspect was observed answering the phone and the surveillance was terminated. Several minutes later the case agent received an incoming call from the suspect asking why he had called him. The case agent was able to convince the suspect he had dialed the phone number in error but was unable to figure out how the suspect had obtained his caller ID blocked law enforcement mobile phone number. It was not until the wiretap was operational that we were able to see the incoming text messages from Trap Call regarding the unblocked incoming calls.

Most government agencies obtain their cell phone contracts under a broad umbrella contract by city, county, or federal entity. Fortunately the suspect in the above case did not have the public records check feature which would have likely indicated the subscriber of the phone was the State of California. Even if the records check did not reveal the name of the investigative agency, it would have seriously hampered the investigation if the suspect became concerned and dropped his phone.

Trap Call has some obvious advantages for law enforcement investigators. However, I see no reason why we should patronize a company which also offers caller ID blocking services and thrives by allowing criminals to mask their identities. The Law Enforcement Telecommunications System from Orion Systems offers the same services, among many others. They are also heavily involved with a number of local, state, and federal law enforcement agencies in a wide variety of investigations. Consider Orion Systems before shelling out personal or department money to a caller ID spoofing company.

Police Technical National Courses

Cell Phone Investigations™ by Aaron Edens

Data from cell phones. Simply the most comprehensive course on cell phone examination and investigations. From the handset to the tower to the phone company to the courtroom.

Craigslist Investigations™ by Wayne Nichols

Methods and tools for successful Craigslist investigations. Case examples include property related crimes, drug investigations, prostitution, and enticement of juveniles.

Digital Forensics and Evidence Handling™ by Andrew E Neal

Data from devices. How the process works, how to handle digital evidence, what not to do, how to win in court, future directions, and building on your own in-house lab.

Excel® for Public Safety™ by Amy Kupiszewski

Harnessing the power of Microsoft Excel® to better manage data and improve investigations. Telephone tolls, financials, arrest stats, fugitive lists and calls for service analyzed with a few clicks.

PowerPoint® for Public Safety™ by Thomas M. Manson

Designed to assist all personnel become more efficient and proficient with PowerPoint® Faster development, internet videos, E911 audio, Splash Screens® and custom animation.

Social Media Methods™ by Doug Nolte

Designed to help departments and their personnel utilize social media effectively to manage their online presence; a prerequisite for any online investigation.

Visit www.policetechnical.com to view the national training calendar

Note: all national classes are two days in length, $350.00 per person, include manual, certificate of completion, and access to additional downloadable material (when applicable)

Bring a POLICE TECHNICAL class to your agency

POLICE TECHNICAL has provided technical training to law enforcement since 1998

In-Service Training

An In-Service is the fastest, most cost effective way to provide technical training to your personnel. We typically provide 2 days of training for up to 40 people at your facility.

An optional 3rd day of training for most classes offers students more hands-on time with the instructor. Simplified pricing includes all expenses: Instructor fees, meals, travel, lodging, and training materials.

Contact our office for rates and scheduling:

812.232.4200 or at info@policetechnical.com

Copyright Information