Prosecutorial Challenges Involving Cell Phones™

Prosecutorial Challenges Involving Cell Phones™ was specifically designed for personnel tasked with utilizing cell phone data in the courtroom. This course derives much of its substance from the longer national course Cell Phone Investigations™ by Aaron Edens. Topics within include: Searching Cell Phones Incident to Arrest, Exigent Circumstances, Overcoming Defense Objections, Locked Handsets, and Problems with Cell Towers.

Aaron Edens
Police Technical

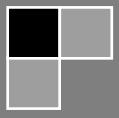


Table of Contents

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.

Goals of the Session

1. Searching Cell Phones Incident to Arrest
    a. Prior Cases
    b. Contemporaneous To Arrest
    c. Current Issues in State Supreme Court
2. Exigent Circumstances
    a. Remote Deletion
    b. Overcoming Defense Objections
3. Locked Handsets
4. Problems with Cells Towers

Session Overview

Technology evolves faster than the law and many current court cases are based on decisions involving pagers. Among the many challenging areas are the authority and the ability to search cell phones, and similar devices, incident to the arrest of a suspect. There are divergent opinions at the Appellate and Supreme Court levels of several states, as well as, conflicting federal Appellate Court cases. It is inevitable that the issue will have to be decided by the United States Supreme Court.

Searching Cell Phones Incident to Arrest

"To say that case law is substantially underdeveloped as to what rights are accorded a cell phone user would be an understatement." United States v. Skinner (E.D. Tenn. 2007) 2007 WL 1556596

Searching incident to arrest is one of the most contested exceptions to the search warrant requirement with respect to cell phones. Beginning with pagers and now extending to cell phones and PDAs, numerous court cases have generally supported the searching of cell phones incident to arrest.

The scope of a search incident to arrest varies based on whether the item searched is an item "immediately associated with person of the arrestee" such as clothing or a wallet, or other personal property near the arrestee, such as luggage. While most people store their cell phones on their immediate person, this illustrates the need to properly and completely document the location where the phone was found (e.g. right front pants pocket, clipped to belt.)

It has not been entirely settled by the courts whether phones are items of personal property similar to a wallet or a closed container of personal property. The Supreme Court stated that "container" should be interpreted broadly to include "any object capable of holding another object. It thus includes closed or open glove compartments, consoles, or other receptacles located anywhere within the passenger compartment, as well as luggage, boxes, bags, clothing, and the like." Subsequently, lower courts have upheld similar searches of wallets, glove compartments, and sealed envelopes.

The typical search incident to arrest has been for physical evidence such as weapons or narcotics. However, the principal has extended to cover non-tangible digital evidence such as evidence of narcotics sales or possession of child pornography. The question is whether data is contained within an electronic device. Lower court decisions have been fairly consistent regarding the searching of electronic devices for non-tangible digital evidence.

Prior Cases

One of the earliest of these cases was a 1993 decision from a federal court dealt with a pager found on a suspect who was arrested as part of a narcotics investigation. The officers found a pager on the suspect and activated the memory to retrieve phone numbers stored inside it. Some of the numbers found in the pager linked the suspect to the narcotics investigation. The suspect challenged the search stating he had a reasonable expectation of privacy in the pager and searching it required a warrant. The court sided with the suspect by agreeing that a pager is analogous to a closed container and that individuals have a reasonable expectation of privacy in the contents of electronic containers. However, the court went on to conclude that because the search of the pager came on the heels of a lawful arrest of the suspect, a warrantless search was permitted under the search incident to arrest doctrine. (US v. Chan ND Cal. 1993) 830 F.Supp 531, 536)

Courts have applied the search incident to arrest exception to cellular phones, including the search of call logs, text messages, electronic address book, and internet inbox. In a 2007 case, law enforcement officers arrested a suspect during a controlled purchase of narcotics. After the suspect was arrested, his cell phone was searched incident to arrest and a cell phone was located in his pocket. One of the officers searched the phone and found text messages related to the sale of methamphetamine. The suspect challenged the search of the phone but the court upheld the search as lawful and stated "police officers are not constrained to search only for weapons or instruments of escape on the arrestee's person; they may also, without any additional justification, look for evidence of the arrestee's crime on his person in order to preserve it for use at trial." US v. Finley (5C 2007) 477 F3 250, 260)

A number of courts have dissented from the search incident to arrest doctrine due in large part to the technological advances in cell phones. In one case, US v Park, frequently cited by defense attorneys, the court noted "due to the quantity and quality of information that can be stored on a cellular phone, a cellular phone should not be characterized as an element of individual's clothing or person, but rather as a possession within an arrestee's immediate control that has Fourth Amendment protection at the station house." At issue in this case may be the fact that the search occurred at the station house and was not immediately contemporaneous to the arrest. United States v. Park, 2007 WL 1521573 (N.D. Cal. May 23, 2007)

The issues raised in US v Park center on the amount of data a cellular phone may contain. While it is true that many of today's cellular phones have significant storage capacity, the courts have failed to notice what is contained within that storage. The mere fact that a cell phone is capable of storing 8, 16, 32, or 64 gigabytes of information may be irrelevant depending on the type of investigation. Most cellular phone forensic examinations I have completed focused on the same fields of data, whether the phone was advanced or not (e.g. electronic phone book, call logs, text messages, etc.). The phones with higher memory capacities were designed to be multi-functional tools, combining the traditional cell phone or personal data assistant with a media player while also allowing for internet access. These devices store memory intensive software applications and media files such as music and movies. In a Nielson survey of more than 4,000 smart phones users the average number of applications on Apple iPhone was 40 . The bulk of these applications were games which can take up a significant amount of memory. Additionally the operating system of the device may take up a significant amount of available memory. The rebuttal to the courts concerns about the advanced storage and computing power of a phone is twofold. First, the amount of storage of these devices is made to accommodate the gaming and multi-media needs of the consumer. Second, regardless of the storage or processing power of the device, most investigators are interested in the same information set available on non-'smart' phones, namely the electronic phone book, call logs, image files, and text messages.

Contemporaneous To Arrest

The time frame of the search appears to be an evolving issue relating to the search incident to arrest exception. Searches incident to arrest must be contemporaneous to the arrest. There is no clear line in the sand as far as the time frame within which this must occur. However, the courts have rejected searches which occurred ninety minutes and two hours and fifteen minutes after the arrest. Similarly, courts have rejected a search which occurred at the station house as not being justified incident to the arrest. The courts have not established an exact amount of time for what contemporaneous is however one case took into account whether officer "conducted the search as soon as it was practical to do so, including whether officers took intervening actions not directly related to the search."

The phone or PDA must have been in the suspect's immediate control when they were arrested, not necessarily when they were searched.

The courts have not fully addressed whether the extensive storage capacities of today's cell phones and PDAs impact searching incident to arrest. As noted earlier, some courts have held that the sophistication or storage capacity of a device is relevant. However, courts have allowed extensive searches of written materials discovered incident to a lawful arrest including, the entire contents of a wallet, photocopying the entire contents of an address book and brief cases .

This is likely not an invitation to spend an extensive amount of time searching a cell phone or PDA but could allow for a warrantless review of the contents of the device to be followed by a more detailed search based upon a search warrant.

Current Issues in State Supreme Court

There's no doubt in my mind that when Ventura County Senior Deputy Victor Fazio reported for work on 4/25/2007 he had any idea his routine buy-bust operation would make State law. I doubt any law enforcement officer would have predicted their controlled buy of six tablets of Ecstasy would make it all the way to the State Supreme Court and may even make it to the United States Supreme Court. Here are the facts of the case as recorded in the Supreme Court case decision:

"About 2:50 p.m. on April 25, 2007, Senior Deputy Sheriff Victor Fazio of the Ventura County Sheriff's Department witnessed defendant Gregory Diaz participating in a police informant's controlled purchase of Ecstasy. Defendant drove the Ecstasy's seller to the location of the sale, which then took place in the backseat of the car defendant was driving. Immediately after the sale, Fazio, who had listened in on the transaction through a wireless transmitter the informant was wearing, stopped the car defendant was driving and arrested defendant for being a coconspirator in the sale of drugs. Six tabs of Ecstasy were seized in connection with the arrest, and a small amount of marijuana was found in defendant's pocket. Defendant had a cell phone on his person. "

"Fazio transported defendant to a sheriff's station, where a detective seized the cell phone from defendant's person and gave it to Fazio. Fazio put it with the other evidence and, at 4:18 p.m., interviewed defendant. Defendant denied having knowledge of the drug transaction. After the interview, about 4:23 p.m., Fazio looked at the cell phone's text message folder and discovered a message that said "6 4 80." (Fazio had to manipulate the phone and go to several different screens to access the text message folder. He did not recall whether the cell phone was on when he picked it up to look through it.) Based on his training and experience, Fazio interpreted the message to mean "[s]ix pills of Ecstasy for $80." Within minutes of discovering the message (and less than 30 minutes after the cell phone's discovery), Fazio showed the message to defendant. Defendant then admitted participating in the sale of Ecstasy. "

"Defendant was charged with selling a controlled substance (Health & Saf.Code, § 11379, subd. (a)). He pleaded not guilty and moved to suppress the fruits of the cell phone search - the text message and the statements he made when confronted with it - arguing that the warrantless search of the cell phone violated the Fourth Amendment. The trial court denied the motion, explaining: "The defendant was under arrest for a felony charge involving the sale of drugs. His property was seized from him. Evidence was seized from him. . . . [I]ncident to the arrest[,] search of his person and everything that that turned up is really fair game in terms of being evidence of a crime or instrumentality of a crime or whatever the theory might be. And under these circumstances I don't believe there's authority that a warrant was required." Defendant then withdrew his not guilty plea and pleaded guilty to transportation of a controlled substance. The trial court accepted the plea, suspended imposition of sentence, and placed defendant on probation for three years." Diaz appealed the decision which was upheld by the Appellate Court finding the cell phone "was immediately

associated with [defendant's] person at the time of his arrest," it was "properly subjected to a delayed warrantless search."

The California Supreme Court reviewed the decision and upheld the search of the cell phone. The Court first addressed the constitutionality of warrantless searches and the exceptions to the Fourth Amendment noting: "One of the specifically established exceptions to the Fourth Amendment's warrant requirement is "a search incident to lawful arrest." (United States v.Robinson (1973) 414 U.S. 218, 224 (Robinson).) This exception "has traditionally been justified by the reasonableness of searching for weapons, instruments of escape, and evidence of crime when a person is taken into official custody and lawfully detained. (United States v. Edwards (1974) 415 U.S. 800, 802-803 (Edwards).) As the high court has explained: "When a custodial arrest is made, there is always some danger that the person arrested may seek to use a weapon, or that evidence may be concealed or destroyed. To safeguard himself and others, and to prevent the loss of evidence, it has been held reasonable for the arresting officer to conduct a prompt, warrantless "search of the arrestee's person and the area "within his immediate control" . . . .' Such searches may be conducted without a warrant, and they may also be made whether or not there is probable cause to believe that the person arrested may have a weapon or is about to destroy evidence. The potential dangers lurking in all custodial arrests make warrantless searches of items within the 'immediate control' area reasonable without requiring the arresting officer to calculate the probability that weapons or destructible evidence may be involved." (United States v. Chadwick (1977) 433 U.S. 1, 14-15 (Chadwick).)

During their review of the case, the Court noted Diaz's objection that the search arguing that the search "was too remote in time" to qualify as a valid search incident to his arrest. In making this argument, the defendant emphasizes that the phone "was exclusively held in police custody well before the search of its text message folder." The Court relied upon three United States Supreme Court cases specifically regarding searches incident to arrest in reaching their decision. The central issues were whether the cell phone was an item of personal property and whether the delay in searching the phone invalidated the search. The Court found: "Under these decisions, the key question in this case is whether defendant's cell phone was "personal property . . . immediately associated with [his] person"(Chadwick, supra, 433 U.S. at p. 15) like the cigarette package in Robinson and the clothes in Edwards. If it was, then the delayed warrantless search was a valid search incident to defendant's lawful custodial arrest. If it was not, then the search, because it was " "remote in time [and] place from the arrest,' " "cannot be justified as incident to that arrest" unless an "exigency exist[ed]."5 (Chadwick, supra, at p. 15.)

We hold that the cell phone was "immediately associated with [defendant's] person" (Chadwick, supra, 433 U.S. at p. 15), and that the warrantless search of the cell phone therefore was valid. As the People explain, the cell phone "was an item [of personal property] on [defendant's] person at the time of his arrest and during the administrative processing at the police station." Because the cell phone was immediately associated with defendant's person, Fazio was "entitled

to inspect" its contents without a warrant (Robinson, supra, 414 U.S. at p. 236) at the sheriff's station 90 minutes after defendant's arrest, whether or not an exigency existed."

While the Court upheld the search there were several issues which were not addressed by the Judges. As the Court had already decided the issue of the search of the cell phone incident to arrest, they did not address the exigent circumstances issue. As noted in the decision: "Given our conclusion, we need not address the People's argument that an exigency existed because a cell phone's contents "are dynamic in nature and subject to change without warning - by the replacement of old data with new incoming calls or messages; by a mistaken push of a button; by the loss of power; by a person contacting the cellular phone provider; or by a person pre-selecting the 'cleanup' function on the cellular phone, which limits the length of time messages are stored before they are automatically deleted." We note, however, that the People have offered no evidence to support this claim. Nor have they offered evidence as to whether text messages deleted from a cell phone may be obtained from the cell phone's provider. (See Orso, Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence (2010) 50 Santa Clara L.Rev. 183, 199 ["text messages are feasibly accessible for about two weeks from the cellular provider"].)

The Court made it clear the prosecution has not admitted any evidence to support the fact that electronic data is perishable from a variety of methods. If the investigating officers or prosecuting attorneys had introduced the wide variety of remote deletion services and applications this could have been avoided. Also, the Court relied on the flawed article published by Orso in the Santa Clara Law Review regarding the availability of text message content from the cellular service provider.

Proper documentation also played a factor in the ruling. In deciding the issue the California Supreme Court also examined the issue of whether the phone was "immediately associated" with the defendant. In their decision the Court found the phone was: "immediately associated with [defendant's] person" (Chadwick, supra, 433 U.S. at p. 15), and that the warrantless search of the cell phone therefore was valid. …the cell phone "was an item [of personal property] on [defendant's] person at the time of his arrest and during the administrative processing at the police station."

The Court also addressed whether to storage capacity of the device was material. In the opinion of the California Supreme Court, it was not relevant. "Regarding the particular focus of defendant and the dissent on the alleged storage capacity of cell phones, for several reasons, the argument is unpersuasive.… neither defendant nor the dissent persuasively explains why the sheer quantity of personal information should be determinative. Even "small spatial container[s]" (dis. opn. of Werdegar, J.,post , at p. 3) that hold less information than cell phones may contain highly personal, intimate and private information, such as photographs, letters, or diaries." Adding "…differing expectations of privacy based on the amount of information a particular item contains should also be irrelevant."

This court case was not unanimous. While the decision clears the way for California law enforcement officers to search suspect's mobile phones incident to their lawful arrest, there are valuable lessons to be learned from the dissenting opinion. In the dissenting opinion Justice Werdegar writes: "Clearly, any justification for the warrantless search of a mobile phone must come from the possibility that the arrestee might, during the arrest, destroy evidence stored on the phone. Once a mobile phone has been seized from an arrestee and is under the exclusive control of the police, the arrestee, who is also in police custody, cannot destroy any evidence stored on it... no evidence of exigency was presented in this case...no evidence that the text messages on defendant's phone were subject to imminent loss and could not, in any event, be obtained from defendant's cellular provider." The Justice further countered the argument of the Attorney General regarding the possibility of remote deletion: "At oral argument, the Attorney General noted that data on some smartphones can be remotely wiped, which might allow an accomplice to destroy evidence on the phone even while the arrestee remains in custody and the phone in police control. As an argument for warrantless searching, this proves too much. A suspect arrested in his or her home or office might also leave behind a computer with evidence that could be destroyed by an accomplice while the arrestee is in custody, but this possibility does not entitle police to search the contents of such computers without probable cause or a search warrant. In either circumstance (home computer or handheld computer) an immediate search without waiting for a warrant might be desirable from the perspective of efficient policing, but "the mere fact that law enforcement may be made more efficient can never by itself justify disregard of the Fourth Amendment." (Mincey v. Arizona (1978) 437 U.S. 385, 393.) In any event, it appears that remote wiping can be avoided by removing the smartphone's battery and/or storing the phone in a shielded container, as law enforcement officers are being trained to do. (See Grubb, Remote Wiping Thwarts Secret Service, ZDNet (Australian ed., May 18, 2010)

I believe the Justice has only a partial comprehension of the issues and practicalities of investigations involving cell phones. It was not included in the record what the model of mobile phone was or who the service provider was, but the Justice seems to be relying on the fiction that text message content is universally available from the cellular service provider. This likely comes from the previously mentioned article in the Santa Clara Law Review. Furthermore, the Justice draws an analogy between a computer left at the scene of an arrest and a cell phone taken as evidence which might be remotely wiped. Standard law enforcement practice would be to secure the computer against possible destruction by an accomplice. Unlike the computer, the evidence on the phone could be destroyed anonymously by anyone as long as the device is communicating with a cellular or WiFi network. The justice relies upon the preventative measures of "removing the smartphone's battery and/or storing the phone in a shielded container, as law enforcement officers are being trained to do." As we will discuss later, the act of removing the battery can actually make a subsequent search more difficult by engaging the handsets password security code. Furthermore, removing the battery can actually change or delete data stored on the device. Additionally, storing the phone in a shielded container is not always feasible for a variety of reasons. The Justice does not specify which container he recommends but the available

devices present a variety of challenges including the fact that they are expensive, and thus not readily available to every law enforcement agency. Also, certain devices are not portable and are designed for use in a forensic laboratory environment. Lastly, to my knowledge, there are no scientific studies of the effectiveness of the various shielding mechanisms. Anecdotal evidence abounds of phones ringing while they are inside shielded materials.

On 9/1/2011 the California State Senate unanimously passed Senate Bill 914. SB 914 would have been codified in California Penal Code section 1542.5 and prevented the search of any portable electronic device, not just mobile phones, without a search warrant. On 10/9/2011 California Governor Brown vetoed SB 914 writing: "The courts are better suited to resolve the complex and case-specific issues relating to constitutional search and seizure protections." As it stands right now, searching a mobile phone or any portable electronic device incident to arrest is lawful. However, this could change rapidly if the California legislature is able to gather sufficient support to overturn Governor Brown's veto.

California Penal Code 1542.5 would have read as follows:

(a) The information contained in a portable electronic device shall not be subject to search by a law enforcement officer incident to a lawful custodial arrest except pursuant to a warrant issued by a duly authorized magistrate using the procedures established by this chapter. (b) As used in this section, "portable electronic device" means any portable device that is capable of creating, receiving, accessing, or storing electronic data or communications. (c) Except as provided in subdivision (a), nothing in this section curtails law enforcement reliance on established exceptions to the warrant requirement.

The section is pretty unambiguous regarding searches of phones requiring a warrant. The law would have also encompassed all portable electronic devices. However, the important aspect was paragraph (c) which would have still allowed searches of mobile devices using established exceptions to the Fourth Amendment. These exceptions include consent, probation, parole, exigency, and abandonment. It appeared this section mainly affects the ability of law enforcement officers to search incident to arrest.

As with the dissenting Justices in the Diaz court decision, the politicians appear to a have a fundamental lack of understanding regarding the realities of preserving and seizing digital evidence. In the statement of legislative intent which precedes the Penal Code section they note:

"The Legislature declares that concerns about destruction of evidence on a cellular telephone can ordinarily be addressed through simple evidence preservation methods…"

The methods involved in the "simple evidence preservation methods" will be addressed more thoroughly in subsequent chapters. However, they are not so simple and there are various drawbacks involved in their use. The dissenting

justices in the Diaz decision felt that shielding materials and other methods were fool proof, commonly available, inexpensive and scientifically proven. Unfortunately, as we shall see, that is not always the case. Each of these impediments will be examined in more detail in subsequent chapters, but in summary the rebuttal to some of the issues raised by the dissenting justices include:

Cost- A shielded examination box can cost up to $1,600 and it is definitely not designed to be portable. Field pouches and bags are available and cost much less, approximately $25-35 each. This may not seem like a significant cost however when multiplied by the number of mobile phones seized by even a small sized agency during the course of a year, the cost can become prohibitive.

Efficacy-Preventing a mobile phone from communicating with a cellular service provider can be accomplished using several different methods but each comes with different pros and cons. The use of shielding materials such as metal mesh, metal foil, metal paint cans such as those used in arson investigations, and the bags and pouches all mentioned above suffer from the same failings. First, there is no scientific study of their efficiency. In other words no one knows with certainty if they actually work and under which circumstances they will fail. There are variables which can affect how efficient a shielding method is including the type of device, the battery charge of the device, and the proximity to a cell tower. The other major issue which arises using shielding materials is that most of the materials actually prevent an officer from knowing if they are actually working. Almost all of the materials are opaque and prevent an investigator from viewing the device to see if the signal has actually been disrupted. Other negative factors involved in using these devices include increased battery drain and the inability to attach a charging or data cable while it is being shielded.

Changing the settings-The most efficient method of interrupting the communication between a mobile device and a cellular service provider is to place the device into standalone or airplane mode. Unfortunately, this requires access to the Settings or Tools menus, which is impossible if the handset security lock is enabled.

Removing the battery or SIM card-Both of these methods work but not every device is equipped with a SIM card. Removing the battery can cause the loss of data and is not possible with some devices such as the iPhone series of devices.

In my opinion the California Legislature failed to consider any of these impediments to properly securing a mobile device before enacting this law.

Due to conflicting Federal and State court cases decisions, it is my opinion this issue will inevitably be reviewed by the United States Supreme Court. Until that time, I recommend search of cell phones and other mobile devices be completed pursuant to a search warrant unless there is an established exception. Due to the inevitable increased scrutiny of law enforcement searches of cell phones I strongly recommend thoroughly documenting the facts and circumstances leading to a warrantless search of a device.

Exigent Circumstances

One of the central issues currently being debated in the courts is the issue of exigent circumstances. The courts are being asked to address whether prior cases involving pager technology apply to today's sophisticated cellular phones and PDA's. The exigent circumstances exemption to the warrant requirement generally applies to the potential for the imminent destruction of evidence on a cell phone. In determining exigency, the following factors should be considered:

The degree of urgency involved

The amount of time necessary to obtain a warrant

Whether the evidence is about to be removed or destroyed

Whether those in possession of the contraband know the police are on their trail

The ready destructibility of the evidence.

In order to substantiate a warrantless search of a cell phone using the exigent circumstances exception, a law enforcement officer should demonstrate the knowledge that electronic data is inherently perishable by a variety of intentional, unintentional, and accidental means. A suspect with even a rudimentary knowledge of how their cell phone works can easily delete text messages, call logs, the electronic phone book, or media files. This can be accomplished in the same amount of time it would take to destroy a paper document.

Remote Deletion

More so than with computers, it is possible for the service provider and/or third party application vendors to offer remote delete services and features. Remote deletion is a process that allows a user to delete some or all of the content of a device remotely using features build into the operating system of the device, a service offered by a cellular service provider, a third party software application, or intentionally sending new data to the device with the intention of deleting older data. Unlike most computers, which may require several affirmative steps on behalf of the user, a cell phone, with cellular, WiFi, or internet service, may constantly be in contact with the provider via the cellular network. There are a variety of provider options for remote deleting of some or all of the content of a cell phone. Third party applications may also offer the ability to delete some or all of the files on a phone. These services were designed to allow a user to remotely delete the contents of their cellular devices in the event they are lost or stolen. As with other technologies designed for legitimate use, criminals may use them to conceal or destroy evidence of their actions.

Sophisticated devices such as those using the Apple or Android operating systems have a number of options for remote deletion. Apple offers a remote deletion option through a free application called Find My iPhone which allows users to remotely perform of number of functions to their phone. These features include activating the global positioning system (GPS) unit to attempt to locate the device, remotely setting the handset pass code lock, and/or remotely deleting the content of the device.

Due to the open nature of the software platform owners of phones using the Android operating system have similar options when it comes to deleting information from a device. There are a number of third party applications, many of which are free, which allow for GPS location, remote locking, and remote deletion of information from the device.

These remote deletion features are not exclusive to higher end devices such as the iPhone and Android phones. Many suspects avoid investing several hundred dollars into a cell phone because it may be seized by law enforcement or stolen by other criminals so they tend to favor low cost prepaid cell phone service providers such as Boost Mobile, Metro PCS, and Cricket. As a relatively new service, Metro PCS and Cricket has added the ability to remotely delete some content from phones serviced by them. At this time the content which can be remotely deleted is limited to the contact list in the electronic phone book. In addition to these provider's policy of not requiring identification from it's subscribers, this remote deletion feature makes these particular cell phone service providers ideal for criminals to use.

Even a non-internet enabled cell phone is susceptible to both low and high tech means of destroying evidence. One method, commonly called "flooding" involves the accomplice of a suspect sending multiple text messages or making multiple phone calls in rapid succession to a device. This causes the older information to be deleted to make way for the incoming information.

The widespread availability of these remote deletion services and features can increase the need for officers to immediately search a cell phone. There may be no easy way of knowing if a seized device is equipped with one of these services or features. As many of these remote deletion features are capable of being activated by a third party, and there may not be any obvious evidence of their existence until the device begins to wipe it's memory clean or the handset lock engages.

Cell phones are also susceptible to a variety of environmental factors including moisture and high temperatures which a computer is unlikely to encounter. More than a computer, a cell phone is easily destroyed or concealed. Additionally, almost every cell phone has a security feature which can prevent a law enforcement officer from accessing it. The simple act of locking the handset with a passcode can make it extremely difficult, if not impossible, to access the basic features of the handset. Due to the huge number of cell phone models and operating systems on the market today, there are no universal tools available for bypassing or unlocking a cell phone handset lock. This differs from computers as there are common tools available for bypassing the basic security including with standard operating systems.

As the courts struggle to address the application of the search incident to arrest doctrine to cell phones, judges have relied on prior cases using some of the earliest communications devices. In a series of cases involving pagers the courts have upheld searches conducted under the exigent circumstances exemption. The courts reasoned that every incoming page caused an older stored number to be deleted.

The courts have recognized similar issues relating to cellular phones , however there is some dissention. Unlike pagers which had a limited capacity for storing data, today's most basic cell phone has an equal or greater storage capacity of the most advanced pagers. This does not limit the possibility of using the exigent circumstances exemption to search a cell phone, but it can restrict the scope of the search. For example, a court ruled the search of a cell phone's address book failed to meet the exigent circumstances exemption because they did not feel the evidence was perishable. When the court issued its ruling, this was likely the case given the technology in use at the time. However, the technology to remotely delete the phone book of that particular phone was likely not in use at the time or its existence was unknown to the prosecution or the investigators.

The courts have recognized exigent circumstances as justification for searching a cell phone where the phone had an option for automatically deleting text messages after one day. However, given today's rapidly evolving cell phone operating systems and the development of third party application, it may be impossible to know simply by looking at the phone or determining the services offered by the cellular service provider whether that particular phone is equipped with that as an option or an as an aftermarket add-on. There are applications which automatically delete text messages after they have been read.

In another case in which the court apparently did not understand the storage limitations of cell phones, the court believed cell phones store text messages until they are deleted by the user and therefore rejected the argument that exigent circumstances justified the search . While true with some very high capacity phones, there are a large number of older- generation or lower- cost models that have significant limitations to the quantity of text messages that may be stored. The same storage limitation applies to the incoming call logs feature on many phones. With some notable exceptions, most cell phones routinely store a limited number of calls based on the manufacturers settings or the memory capacity of the device.

It is important to distinguish that when exigent circumstances may support the seizure of a phone, they do not always allow for the search of same. The need to seize a phone to prevent destruction of the evidence does not necessarily authorize law enforcement to take further steps without a warrant.

Overcoming Defense Objections

Defense attorneys may challenge the exigent circumstances exception based on the volatility of the electronic data. One legal scholar refers to it as "...a budding legal fiction in the application of the exigent circumstances exception...that an exigency exists merely because information is stored on a cellular phone." The author of the article, Matthew Orso, believes because cellular service providers keep records of incoming and outgoing calls this eliminates the exigency which may result from the potential loss of information from the phone. Furthermore, based on a news article citing a single cellular service provider, Orso believes text messages are stored for "roughly two weeks" and this "leaves more than adequate time to obtain a warrant and serve it upon the cellular company." In my opinion the "budding legal fiction" is contained in Orso's article and unfortunately is becoming a 'fact' cited by other attorneys, and most recently the California Supreme Court. This is a dangerous misunderstanding of how cellular phones and cellular service providers operate and could perpetuate unless it is addressed.

Orso states text messages are stored for "roughly two weeks" but lacks a clear understanding of the differences between the various cellular service providers and attempts to establish an arbitrary standard for text message storage of two weeks based on one company's, now past, practice. At the time, Orso used as an example one cellular service provider (Sprint) who at the time stored text message content. That company no longer stores text messages content, and in fact, very few do.

Orso fails to note that despite the demands for compliance by a specific date, many cellular service providers routinely take several weeks or longer to provide the information from a search warrant or other legal process. This can significantly delay an investigation when an officer is forced to wait an indeterminate time to receive the responses from their legal process. For many investigations, the mere fact that a delay in obtaining the records is inconvenient is

insufficient to justify an exigent circumstances search of a cellular phone. However, certain crime types lend themselves to an increase in the exigency. Some significant crimes against persons (rape, homicide, etc.) may increase the emergency requirement to obtain the information in minutes or hours instead of weeks or months.

Orso failed to note information returned from the cellular service provider only lists the phone numbers dialed or received and does not store the user supplied identity which accompanies the entry in the phone book. The significance of a phone number may be lost on an investigator until he or she determines it was stored in the phone book using a gang moniker, nick name, or the full or partial name of a subject. As criminals are fond of using prepaid or pay as you go services which do not require the verification of the subscriber's identity, this may be the only opportunity to capture the information. Additionally, obtaining this subscriber information requires a second round of court orders or search warrants to attempt to obtain the information obtained from the results of the first court order or search warrant on the targeted phone number. This can add weeks or months to an investigation.

As stated, Orso fails to note that currently only a small number of the cellular service providers store text messages content. The duration of the storage may be determined by the server storage capacity of the provider and not a finite number of days or weeks. In most cases once the text message is delivered it is no longer stored on the cellular service providers computers. In another troubling topic, Orso further discusses the ability to forensically recover deleted text messages from the subscriber identity module (SIM) of a GSM phone. While it is possible to recover a limited number of deleted text messages from a GSM phone, the number of messages which can be recovered is not infinite. Orso's article is dangerous because it is filled with inaccuracies or partial truths which both the prosecution and the defense may rely upon as fact.

Now that law enforcement is aware of remote deleting services and the technological limitations of preventing a cellular phone from communicating with the network we may be able offset some of the defenses' objections to an exigent circumstances search of a phone. It is established that the courts may consider a law enforcement officers training as to the meaning and significance of facts if the opinion was based on the officer's training and experience and appeared to be reasonable. An officer's opinion may be considered even if he or she is not qualified as an expert witness in court. It is important for an officer to document their training and experience in their reports and search warrant affidavits. An example of one such report is included with this manual. It should be used as a guideline or template and not simply copied verbatim.

If a law enforcement officer is going to seize and search a cell phone using the exigent circumstances exemption to the warrant requirement, they should take steps to attempt to secure the phone from communicating with the network. The simple belief or assertion that exigent circumstances to search may exist, without taking steps to prevent the possibility of remote deletion, fails to substantiate the exigent circumstances claim.

Locked Handsets

What is a locked handset? In relation to cellular phones, the term 'locked' has two primary different meanings. Within the cellular telephone industry, the term refers to restricting a cellular telephone to a particular service provider. This allows a provider to recover subsidies used to entice consumers into purchasing an expensive handset. The more common meaning of 'locked' refers to activating a security features which requires entering a password, pass code, facial recognitions features, or tracing a pattern on the screen of device in order to unlock it. It is widely believed that engaging the security features of a mobile device demonstrate a higher expectation of privacy on behalf of the user.

An important distinction, which has not been adequately addressed by the courts, is whether the routine swipe feature designed to prevent accidental dialing is considered a security feature. In a Northern California case, the ACLU and the Electronic Frontier Foundation tried to assert the feature is a security device indicating the user has a higher expectation of privacy and requiring a search warrant. However, these types of locks are more commonly used to prevent the user from making accidental calls such as those commonly referred to as "butt dialing".

It is estimated that approximately 30% of cellular phone users routinely engage their cell phone's security features. However, these estimations do not differentiate between citizens and criminals and the anecdotal experience of many forensic examiners is that approximately 50-70% of suspect phone submitted for evidence retrieval are handset locked.

Cellular phones with the handset security feature are particularly vexing for forensic examiners. Some operating systems and/or models of cellular phones require alteration to some of the device's settings which allow standard forensic equipment to communicate with the device. Without those changes to the operating system, many of the more common forensic tools will not work. Due to the increased time and resources necessary to bypass the handset security features, as well as, the higher expectation of privacy, it is recommended searches of locked cell phones be accomplished pursuant to a search warrant.

While there are technological methods to bypass almost every mobile phone's security features, given sufficient time and resources, the most common method is simply asking the owner for their password, code, or pattern unlock. However, a recent federal court found obtaining a password from a suspect was testimonial and must be preceded by a Miranda admonition. U.S. v. Rogozin, 2010 WL 4628520 (U.S. District Court for the Western District of New York 2010)

Problems with Cells Towers

For the last several years cell tower data has been used in the prosecution of criminals in the United States. However, some of these early cases were predicated upon less than complete information. That legacy has come back to haunt law enforcement and prosecutors as they try to rehabilitate prior incomplete information. Some of the more common problems encountered with testimony regarding cell towers, include:

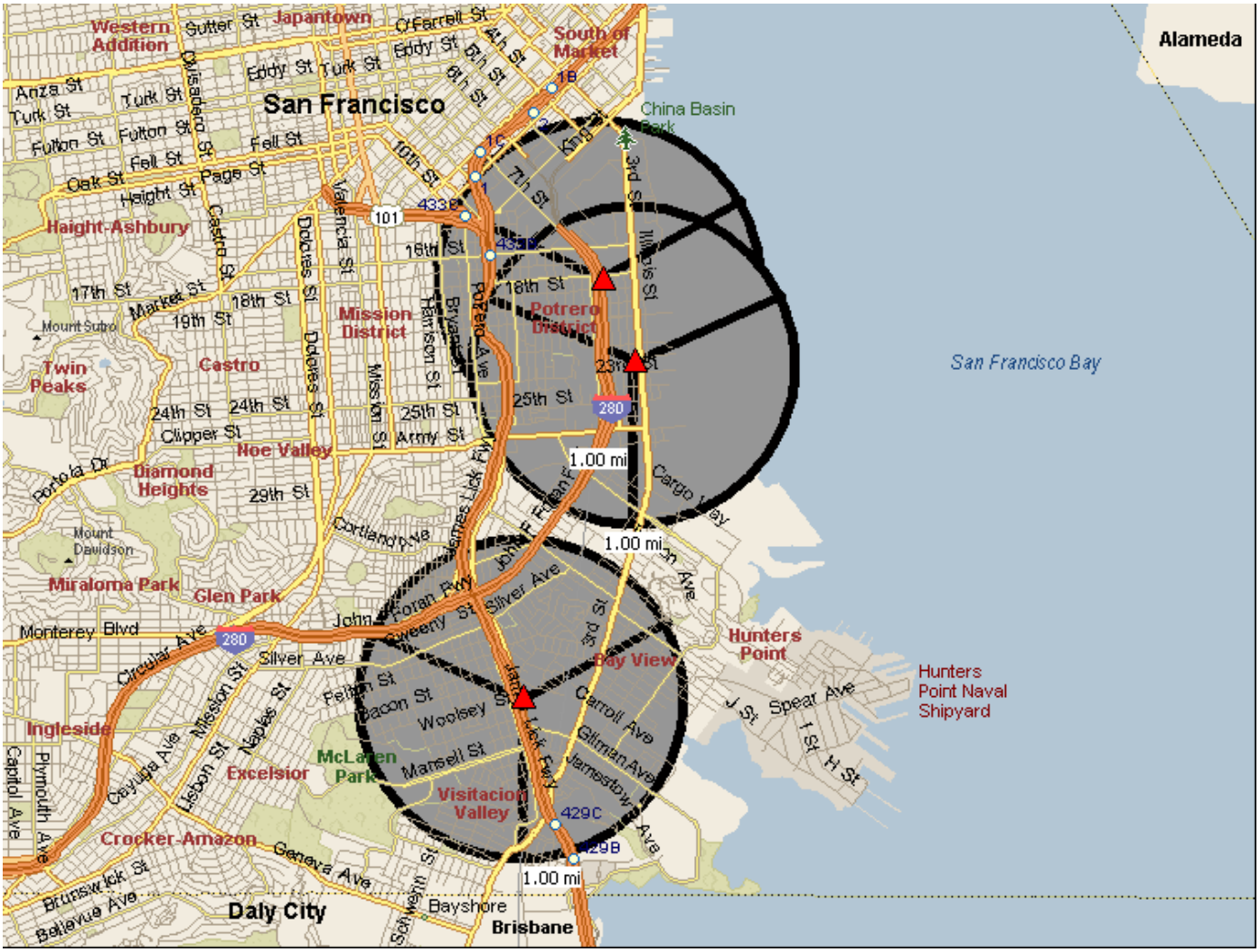
Failing to request or preserve cell tower data early in the investigation

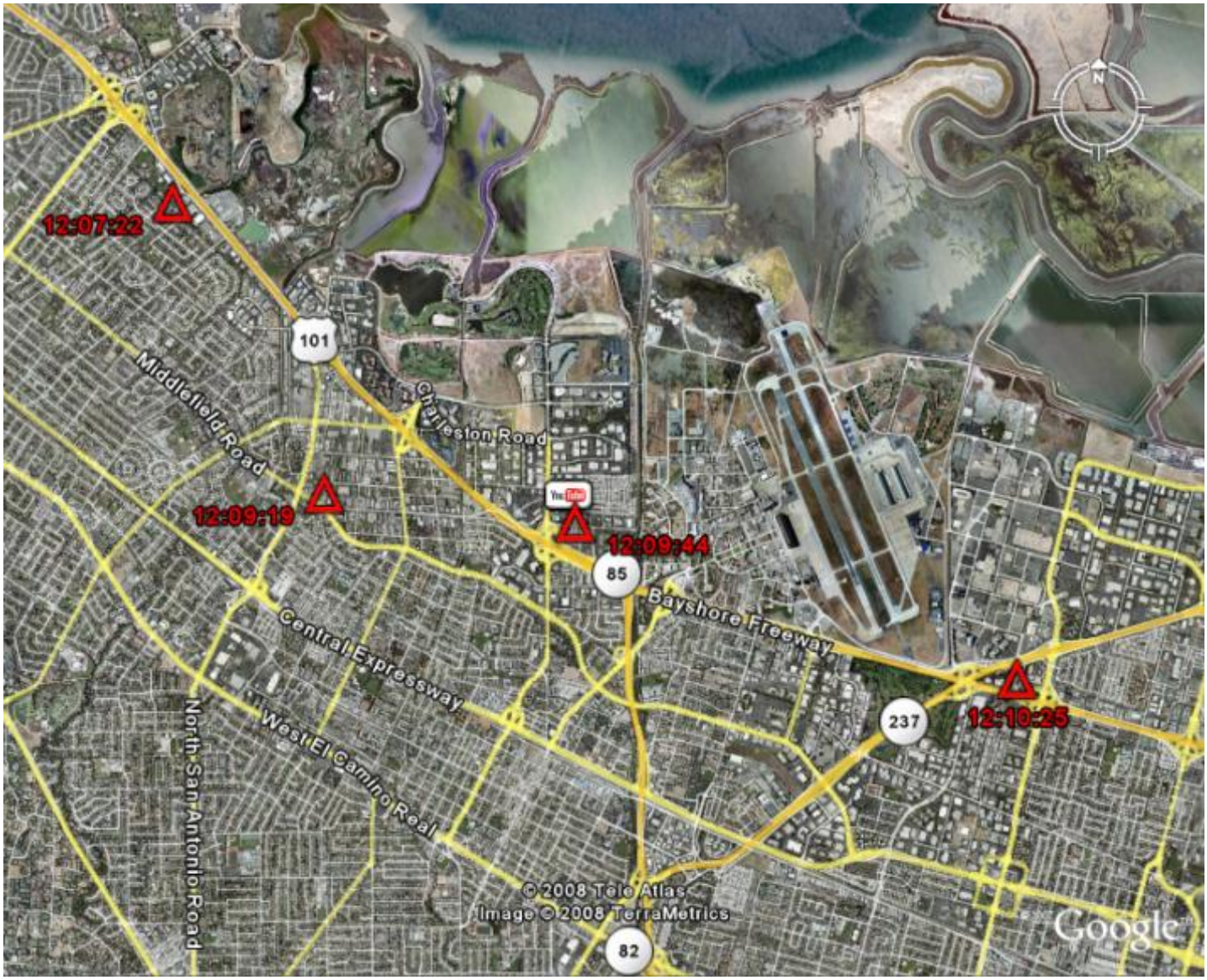
Presuming the communicating tower is the closest and not the tower with the best signal

Using the cell phone location and the suspect location interchangeably

Trusting the theoretical layout of cell tower antennas

Failing to note the azimuth of the tower


Western Addition
Japantown
South of Market
San Francisco
Alameda
China Basin Park
Haight-Ashbury
Mission District
Potrero District
Twin Peaks
Castro
Noe Valley
Diamond Heights
Miraloma Park
Glen Park
Ingleside
Excelsior
McLaren Park
Visitacion Valley
Crocker-Amazon
Daly City
Bayshore
Brisbane
San Francisco Bay
Hunters Point
Hunters Point Naval Shipyard
Bay View
1.00 mi
1.00 mi
1.00 mi
101
280
280
Mount Sutro
Mount Davidson


12:07:22
101
Middlefield Road
Charleston Road
12:09:19
12:09:44
85
Bayshore Freeway
Central Expressway
West El Camino Real
North San Antonio Road
237
12:10:25
© 2008 Tele Atlas
Image © 2008 TerraMetrics
82
Google

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