Cell Phone Records – Training Materials

A1

- 3729 -
Cell Phone Records

Training Materials
Tuesday, March 16, 2010

8:00-9:00  REGISTRATION/ROSTER SIGN IN *(All course participants)*

9:00-9:15  WELCOMING REMARKS

9:15-10:15  CASE LAW UPDATE

10:15-10:30  Break

10:30-11:30  JOINT FINANCIAL INVESTIGATIONS WITH CDCR

11:30-1:00  Lunch Break

1:00-3:00  CELL PHONE EVIDENCE

3:00-3:15  Break

3:15-5:00  CHINA CONNECTION: AN EMERGING MONEY LAUNDERING TREND

***Attorneys & Paralegals required to sign out for MCLE credit***
**Cell Phone Class**

**How to get the Good Stuff**

**Typical Cell Phone Questions**

- What do I need to get a cell site tower location?
- How can I see if a phone is registered on the network?
- Can I look at a phone w/o a search warrant
  - for the purpose of determining its number
  - for the further purpose
    * of writing a search warrant for the service provider
- What if provider drags its feet complying w/ SW
  - Any recourse
  - Any recourse after the fact
- Costs of records

**Cell Phone Records**

- Where is the Evidence
  - Cell Phone
    - Search Warrant
    - Search Incident to Arrest
  - Cell Phone Historical Records
    - Search Warrant
    - Subpoena
  - Cell Phone Real-Time Information
    - Tracking
      - Search Warrant
      - Subpoena
    - Writings
      - Search Warrant?
      - Subpoena?
  - Billing

**Olmstead v. United States**

Q. when was this written

- Subtler and more far-reaching means of invading privacy have become available to the Government.
- Discovery and invention have made it possible for the Government... to obtain disclosure in court of what is whispered in the closet.

**Searches**

- 4th Amendment “Search” requires
  - Search Warrant
  - Exception to need for Search Warrant
    - Exigent circumstances
    - Consent
    - Search Incident to Arrest

**Search Incident to Arrest**

- Chimmell — Search Incident to arrest must be justified by
  - Danger to arresting officer — reaching distance
  - Preserving evidence
- Belton
  - In a car: reaching distance = interior of car
  - Predominantly understood to mean
    - area reachable by arrestede b4 arrest,
      - Brennan dissent: rests on “fiction... that interior of car is always within the immediate control of an arrestee who has recently been in the car”
    - even if currently in back of police car

**Searches**

- 4th Amendment “Search” requires
  - Search Warrant
  - Exception to need for Search Warrant
    - Exigent circumstances
    - Consent
    - Search Incident to Arrest

**Search Incident to Arrest**

- Chimmell — Search Incident to arrest must be justified by
  - Danger to arresting officer — reaching distance
  - Preserving evidence
- Belton
  - In a car: reaching distance = interior of car
  - Predominantly understood to mean
    - area reachable by arrestede b4 arrest,
      - Brennan dissent: rests on “fiction... that interior of car is always within the immediate control of an arrestee who has recently been in the car”
    - even if currently in back of police car

- 3732 -
You want it, You Gotta

- $50 for call detail more than 15 days
- $10 for each additional payment sheet
- $20 for call detail reports exceeding beyond the credit order date
- 250 for call detail reports exceeding beyond the credit order date
- $300 for call detail reports exceeding beyond the credit order date
- $300 for call detail reports exceeding beyond the credit order date
- $200 for CDR changes for per request and/or wire tap

Call Detail Records ATT Example

How Much Does All This Cost

$$$$$$$$

Billing Practices of ISPs

- Federal
  - ECPA
    - requires reimbursement for costs reasonably necessary for producing the records.
    - All orders are treated as a form of compulsory process under the ECPA
  - But
    - Ca. Evid 1563
    - A memorandum on billing and
    - An argument can be made that the State of California has foreclosed the possibility of
      a recoverable
2703(d) Articulable Facts Order

**ECPA Requirements**

- **Order**
  - Notice to Subscriber, unless ...
  - Signed by a Court,
    - includes State Judges
    - "specific and articulable facts showing reasonable grounds to believe that the ... records or other information sought, are relevant and material to an ongoing criminal investigation."

**Provider Records**

**Stored Transactional Information**

- A search warrant or a 2703(d) order will get you:
  - Basic Subscriber Information
  - Complete audit trails/logs
  - Web sites visited
  - Identities of e-mail correspondents

**Basic Subscriber Information**

- A search warrant or subpoena will get you:
  - Name & address
  - Local and long distance telephone toll billing records
  - Means and source of payment used to pay for the account
  - Telephone number or other account identifier (such as username or "screen name")
  - Length & type of service provided
  - Records of session times and durations
  - Any temporarily assigned network addresses

**So What Can I Ask For?**

- **Billing Records**
  - *do not ask for toll information; that is a landline term for long distance.*
  - Specify period desired.
- **Outbound and Inbound Call Detail**
  - *this is the real time, current activity that is not yet on the customer's bill.*
  - "Inbound" is usually available for only a limited time (45 days) which gives other cellular phones calling the target number.

**Keep Your Investigation Secret**

**2705 Non-Disclosure Order**

**NON-DISCLOSURE ORDER**

It is further ordered that cellular service provider not to notify any person (including the subscriber or custodian to which the records relate) of the existence of this order for 90 days in that such a disclosure could give the subscriber an opportunity to destroy evidence, notify confidantes, or hinder or continue his flight from prosecution.

18 USC 2702 (Pen/Eff), 18 USC 2705

**So What Can I Ask For?**

- **Call origination / termination location.**
  - Available for a limited time (45 days) and gives location information on cell sites used, length of call, date, time, numbers dialed.
  - With a GPS enabled phone gives location of phone.
Has the Number Been "Ported"
www.nationalpooling.com

Now that We Know the Carrier

• Where do we serve the paper
• Resources
  - www.mobileforensics.info
  - www.search.org/programs/hightech/spdfse/dl.asp

SW/SDT's
www.mobileforensics.info
Monitoring Tracking Device

- Monitoring
  - Public Places
  - Private Places
    - I.E. beeper reveals info not available to naked eye
    - Needs a SW
- Question
  - How do we know where the tracker is going to go in advance?

Using a phone as Tracking Device

- Pen/Trap Trace
  - Legal standard, articulable facts (Pen Register)
    - Pen registers are available upon "articulable facts." 18 U.S.C. 2703 (aka EFOA), 3127(3) aka (patriot act)
    - But, pen register information "shall not include physical location of the subscriber." 47 U.S.C. 1602(a)(2)(B) (Communications Assistance for Law Enforcement Act aka CALEA)
  - Therefore, need Probable Cause - SW
    - California, cell phone specifically exempted from pentrap

Tracking Summary

- Pen Trap/Trace or Register (if it is a calling that it)
  - Residential Phone, Articulable Facts 2703 order, Pen/Trap Register
  - Cellular Phone
    - Technical - Articulable Facts California, U.S.
  - Location information of cellular phone (not phone is there)
  - Real Time (Trap/Trace) -
  - SW
  - Historical Records -
    - SW, or possibly 2703 order
  - Contents of communication
    - Call + whatap
    - Text/E mail
      - California SW
      - Federal SW
      - Articulable facts order for "spying" E mail

What are the Steps to Get the Stuff

- Identify the target phone number
- Identify the ECSP (Cell Carrier)
- Locate where to serve the SW
- Write the SW
- Serve/Pay for the SW/Records

Who is the ECSP

- 1. What carrier is the phone number assigned to?
  - NANPA - North American Number Pooling Admin
    - www.nationalnanpa.com
- 2. Has the number been ported?
  - National Pooling Administration
    - www.nationalpooling.com

NANPA
www.nationalnanpa.com
So What Can I Ask For?

- Physical address of cell sites.
  - Needed to determine where cell site is located when you receive: inbound & outbound or call origination & termination location.
- Any other cellular telephone numbers that dial the same numbers as (xxx) xxx-xxxx.
  - If you want to know who calls the same number the target calls (for example a pager or landline number).
  - Available for only a limited time (45 days).

So What Can I Ask For?

- Subscriber information on any cellular numbers that (xxx) xxx-xxxx dials.
  - Subscriber information on the carrier’s network that is dialing the target.
- All of the above records whether possessed by cellular service provider (target of warrant) or any other cellular service provider.
  - If you anticipate the suspect may be roaming or if the number is roaming in the providers market, you may be able to obtain information from other cellular carriers if you include this language in your description of need.

So What Can I Ask For?

- All stored communications or files, including voice mail, email, digital images, buddy lists, and any other files associated with user accounts identified as: account(s) xxxxxxx, mobile numbers (xxx) xxx-xxxx, or e-mail account roe1234@sprint.net.
  - Cellular service providers now offer similar services to an Internet service provider (ISP) and maintain the same type of records such as text messaging, e-mail, and file storage for the transfer of data including digital pictures. Limit your request to what you need.

Is a phone a Tracking Device

- Enhanced 911
  - By the End of 2005 Providers must pinpoint
    - 67% of calls within 100 meters
    - 95% of calls within 300 meters
  - 47 C.F.R. 20.18(h)(1)

Installing Tracking Device

- Installing
  - Particularity - hard to specify where beeper will go
    - Describe object beeper placed in
    - Describe object installation which and to installation
    - Describe length of time beeper will be monitored
  - Inside Items, xio 3W
    - Consent of "current" owner to be used by 3rd party target
    - Placed inside a lawfully opened mail parcel with drugs
      - 3 W., P. v. S.W. (1992, 177 Cal.App.3d 1001, 219) (opening SW did not have any language regarding placing 3rd party)
  - Into/OncVehicles
    - Cash
      - No SW necessary
    - Inside
      - Requires a SW

Location/Tracking

SW v. Articulable Facts

- Installing
- Monitoring
- Use of Cell Phones to Track
Where to Find ECSP Records

SEARCH.ORG

What Do the Records Look Like

Call Detail Report

Tower Records

Example - 7/1/07
Fraud Occurs in Palm Beach Fla at 1:12 PM

Q - Can I use Cell Tower Info to establish ID
Belton

Lower courts began to treat ability of police to search interior of car incident to arrest as an "entitlement"

Indeed, arresting officer in Arizona v. Gant - Q. Why was the search conducted - A. "Because the law says we can do it."

Search Incident to Arrest
Arizona v. Gant 173 L.Ed.2d 485

- Search Incident to Arrest OK
  - 1. Danger to Arresting Officer
    - But, no danger if arrestee is handcuffed in back of car
    - I.E. danger is measured at time of search, does not relate back to earlier time of arrest.
  - 2. For Evidence Related to Crime of Arrest
    - "when it is reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle"
    - Q. Isn't that the same as - Probable cause
      - Escalating probable cause

Using a Search Warrant

- SW requires
  - Particularity of place and items searched for
    - How do you describe a cellphone
    - How do you articulate what you want
      - For the court
      - For the electronic communications service provider (ECSP)
    - Describe evidentiary relevance
    - State the training/experience relied upon
    - State conclusion
      - "I believe, based upon my training and experience, that relevant information is contained within the telephone"

Getting a Search Warrant

- SW requiring
  - Particularity of place and items searched for
    - How do you describe a cellphone
    - How do you articulate what you want
      - For the court
      - For the electronic communications service provider (ECSP)
    - Describe evidentiary relevance
    - State the training/experience relied upon
    - State conclusion
      - "I believe, based upon my training and experience, that relevant information is contained within the telephone"

Getting the Phone Itself

- Describing the Phone
  - Physical Description - color, manufacturer, model, etc...
  - IMEI Number - 123456789012345
  - ESN
  - SIM Number

- § 2703(f) Requests to Preserve
  - Can ask for anything (content or non-content) to be preserved for 90 days
  - Does not have prospective effect
    - Applies only to materials in the possession of the provider at the time of the request

- 2d Step Search Warrant for the records
  - Feds and some other states allow some records to be obtained with less than probable cause
  - California, basically requires a SW
  - SW will get records, stored communications etc...
  - Include "Non-Disclosure" language in SW affidavit

- Get Info From the Phone Company
  - Step "freeze" the records
    - 18 U.S.C. 2703(d and f) orders, direct 3d party ECSP
    - Maintain records for 90 days
    - Not disclose the investigation to suspect
  - 2d Step Search Warrant for the records
    - Feds and some other states allow some records to be obtained with less than probable cause
    - California, basically requires a SW
    - SW will get records, stored communications etc...
    - Include "Non-Disclosure" language in SW affidavit

- § 2703(f) Requests to Preserve
  - Can ask for anything (content or non-content) to be preserved for 90 days
  - Does not have prospective effect
    - Applies only to materials in the possession of the provider at the time of the request
ECPA Billing Contd.

What is a “Reasonable Amount”

- ECPA states the amount of the fee is to be mutually agreed upon.
  - If no agreement, amount to be determined by the court that issued the order.
- What is a reasonable cost in California, see E.C. 1563(b)(1):
  - $.10 per 8½ by 11 sheet of paper
  - $10.00 per hour of clerical time
  - Actual costs if provider reimburses a third party for records held by 3rd
    - Does not apply if 3rd is a division of the provider in re Marriage of Stephens
    - 0.00 for computer costs in re Marriage of Stephens (1984) 156

Thank You

- Questions
Why do people need text messaging on cell phones? I don't need it. I can send text messages on my cell phone if I want, but I don't want. I do realize that it has become a sort of life support system for kids; if they're not talking on their cell phone, they are holding it and text-messaging up a storm. An investigator's life would be so much better if there were no such thing. Since text messaging (aka SMS-Short Message Service) appears to be here to stay and some (lots of?) bad guys use it, we'd better learn what it is, how it's used, and how we can legally obtain information about its use to support our investigations.

What does Short Message Service (SMS) mean? It's called "Short" because there is a limitation on how many characters you can put in a message. This is necessary so that the cell companies can easily handle the traffic. If you have SMS service on your cell phone, you type an alphanumeric message using your keypad and then "send" it to your intended recipient. If the recipient's phone is on, s/he can view the text you have sent. Obviously, text messaging is a one-way affair, much like push-to-talk.

Where and how it's stored and for how long: This is probably the most misunderstood issue regarding SMS. I have received many calls from investigators who have been informed that a particular text message was sent last week/month/year - you name it - which could have a major impact on a case. If only they could somehow subpoena the text of that message, the case could be resolved. They don't like it when the cell company tells them that the text message is long gone and irretrievable. This is usually when the call me and ask if there is some way they can get the contents of that message; I have to tell them the bad news and verify that what the cell company told them was correct. The life of a text message is, sadly, very short; here's the sad tale...

When a text message is sent, it goes to the cell company's text message server where it is temporarily (for seconds) stored. The cell company communication system checks if the recipient's telephone is turned on. If it is, the text message is sent and, within a short period of time (typically minutes or seconds) is deleted from the cell company server. The message is now resident on the recipient phone's memory. It will stay on the recipient's phone until s/he deletes it or it gets automatically "bumped off" when the phone's text message storage memory is exceeded and the phone needs to make space for a new message.

If the intended recipient's phone is turned off, obviously the message cannot be sent and it is retained for a short period (most cell company systems hold it for 72 hours - three days) on the server while it is waiting for the recipient phone to be turned on. If 72 hours has passed and the recipient phone has not been turned on, most cell companies delete it permanently and it is lost forever. At least one company representative told me that in their system, the message would be...
transferred after 72 hours to an archival system where it will wait for an unspecified period (around a month or so) for the recipient phone to be turned on. After that period has passed, it will be deleted. I have not been able to verify if this information is accurate; you should assume that it is kept for only three days and then deleted. As always, I recommend that before you write your legal demand, call the cell company compliance department and find out their policy.

**Getting SMS traffic and content:** You might think of SMS information as being analogous to telephone call information. You can get tolls (aka call detail records – CDRs) for telephone calls. CDRs give you information such as the date, time and duration of a call and what number called what other number. If you want to know what the people talked about, i.e. you want to listen to the conversation, this requires additional justification, legal paper, and equipment, but Title II intercepts can be and are regularly done on both landline and cell phones.

With an SMS text message, you can get the equivalent of CDRs – who sent a message to whom and when. Remember the comment I made earlier – text messaging is only one way. Consider this. If you introduce subpoenaed information at a trial that shows Subject A sent 35 text messages to Subject B on a given day, and you didn’t subpoena Subject B’s SMS records, couldn’t Subject B’s attorney argue that Subject B’s phone was off for several days and he never received them? Or couldn’t learned counsel argue that his client might have seen the messages, but didn’t recognize the sender and just deleted them? You’re on the stand; it’s too late to serve another subpoena! Lesson: get both sides.

If you want the actual message content – the equivalent to Title III, and you can generate the appropriate legal paper, you can get it only in real time in a Title III CALEA Intercept. On all occasions where I have had to get text message information, each and every cell company has stated emphatically that the only way to get content is via a CALEA intercept and only in real time.

Remember that if you want to show that two people were communicating via text messaging, it will be necessary to subpoena or otherwise legally capture both sides of the SMS "conversation" and put them together to show the extent of the dialog. Otherwise, if you only look at only one subject’s SMS information, you will just be able to establish a monologue in court.

Bottom line is, if you want SMS traffic information, you have all kinds of time. If you want SMS content, i.e. the actual text of the message, you have to plan ahead for the necessary legal paper and grab it real time.

Of course, if you can get your hands on that cell phone and you have the appropriate legal paper, you can read any messages that have not been deleted. Even if a message has been deleted by the recipient and not much time has passed, you may be able to recover some or even possibly the entire message forensically.

OK, OK, OK, there are a couple of other options. The above discussion covered the 99+ situations you will encounter. There are two circumstances that could occur. Both possibilities are unlikely, but I would be amiss if I didn’t mention them.

- **Way out possibility #1:** If you know an SMS was sent to a particular cell phone on a certain date/time and if you know that the message was never received because the recipient cell phone was turned off, and if it has been less than 72 hours since the message was sent, that SMS is still sitting on the cell company’s server. Even if you have a court order for a CALEA Title III, you still can’t read the message because the recipient cell phone is off so the SMS will never be sent and will die a natural death after the 72 hours is up. Your only solution is get the cell company to copy, extract, freeze, or do whatever they have to do to retrieve that message before it dies. Thy will tell you it can’t be done or they may tell you
they just won't do it. Don't believe them; it can be done; you just have to exert the proper amount of legal and “other” force (refer to your telephone force continuum training) to make it happen. Just do what you have to do before the 72 hours is up. (Idea... have them set up a done cell phone to the one that's turned off. When the clone is turned on, the SMS will be sent.)

- Way out possibility #2: If “Way out possibility #1” happens and, if the 72 hours has passed but only by a very short time (minutes or maybe just an hour or so), and if the situation is exigent, and if you have the mental fortitude, legal paper, and determination, you could always execute a search warrant at the cell company office, grab their SMS server and possibly recover the deleted SMS forensically. Actually, if the cell company wanted to help, they could do all that for you, but as you know, their first responsibility is to their shareholders. If you do exercise this option, let me know how it turned out!

If you like the clone phone idea mentioned above and you are a covert operator with a “Mission Impossible” bent; a great trick is to remotely “shut down” a subject's cell phone by using a Triggerfish-type unit (the latest man-portable version is the “Kingfish”). Appropriate legal paper should get the cell company to build you a clone of the shut-down phone. Then you could receive all the text messages that would have been sent to that subject (and you could even respond to them). Just be sure you keep his phone shut down.

**Selected short subjects:**

**You don't forget your buddies; don't forget the bad guy's buddies:** Sprint, to name one, and lots of other cell companies offer special deals to customers who have a small, select group of people that talk to each other a lot. The advertising types call it the “buddy” plan, “friends and family” plan or some other catch phrase, but they all basically work the same. I guess they do it to encourage groups of people to all sign up together and all stay with their company. For example, when you and a group of friends apply for Sprint cell phone service, you can ask that you and your buddies be put on the “buddy plan” so that calls between any two members of the group are at the bargain rate. Some cell companies allow free calls among members of a “buddy” plan. What a great way to find out quickly who all your target’s close associates are! Not all bad guys are stupid enough to put a list of their co-conspirators on file, but enough of them do it to make it worthwhile for you to include a request for a target’s “buddy list” in your subpoena. Note that this doesn’t work for Verizon Wireless — they don’t charge minutes for “in-calling”, communication between any Verizon Wireless customers.

**Some telcos will email you a spreadsheet instead of paper if you request it?** Isn't that great! Now you can easily dump the calls into your analytical system or at least sort and study them on the spreadsheet. No more fat-fingering for you. Don’t you wish all telcos would send all info this way? So far, I’m in agreement with you. Electronically-delivered tolls do save a lot of time. But you need to be aware of a possible disaster that could blow your case. Let’s look at a scenario. You take the stand at the trial and testify that the defendant called his alleged co-conspirator (whom he claimed he did not know) 237 times during the past four months. You sit there all smug while the defense attorney springs his planned strategy on you. He claims that his review of the discovery information that you provided revealed that the telco you subpoenaed emailed you the tolls on his client’s cell phone in a Microsoft Excel spreadsheet. How, he asks, can you expect the jury to believe that 237-call figure you quoted when anyone knows that you could have easily edited that spreadsheet to show anything you wanted in your efforts to frame his poor, innocent client? You may want to think twice about introducing evidence that could be challenged in this manner. Sure, get spreadsheet format call and/or subscriber records for your analytical/investigative
convenience, but when you go to court; be sure you have a parallel set of original, from-the-telco paper or read-only, graphic subscriber and call detail record information to introduce as evidence. For all practical purposes, if you have a CD from the telco with some sort of "official" telco logo on it, you’re good for court.

The only thing we have to fear is fear itself... Here is an email I received recently:

JUST A REMINDER!!! .... 9 days from today, all cell phone numbers are being released to telemarketing companies and you will start receiving sale calls.

..YOU WILL BE CHARGED FOR THESE CALLS - To prevent this, call the following number from your cell phone: . It is the National DO NOT CALL list. It will only take a minute of your time. It blocks your number for five (5) years. You must call from the cell phone number you are wanting to have blocked. You cannot call from a different phone number.
Thought you may want to know this...
~Nora

Fear not: this has all the earmarks of an urban legend. I think you are wasting your time registering. No one will be releasing cell numbers to telemarketers. If you do register your number I don't think it will make much difference; FCC does not enforce the Do Not Call law! In fact, no one enforces this law and the telemarketers know this. The only reason any of them honor this list is because they are afraid of more stringent laws that will be enforced if they don't act honorably. FCC does, however, release the Do Not Call list to telemarketers so they'll know what numbers they are forbidden to call. Many unscrupulous (are there any un-unscrupulous telemarketers?) telemarketers use this list to make calls, particularly those from safe, overseas telemarketing boiler rooms.

This being said, if/when a national 411 directory of cell phone numbers is published, it will not be distributed as such, but will be only given out on a specific query basis - i.e. you give them a name and they give you the number.

My advice... if you're worried about such a release ask that your number be non-published. As far as telemarketers are concerned, wait until you get a call - then register. Never call a telemarketer back.

---

NTI publishes "a monthly newsletter written by analysts, and prosecuting attorneys. A sworn law enforcement officer provides direct assistance regarding telephone issues to federal, state, and municipal agencies. He also conducts in-depth, training programs for investigators, prosecutors, and analysts either directly or off the GSA schedule for federal agencies on using telephone information to support criminal and counter-terrorism investigations. Each issue covers techniques and innovative approaches to the acquisition and use of telephonic information to build and prosecute cases. Call if you have any questions or want more detail on the information presented here. The material presented may not be reproduced and/or distributed in whole or in part without the express permission of the author. Previously unpublished investigative and analytical techniques presented herein may not be used by any person or enterprise for commercial purposes.
Cellular phones have become the virtual biographer of our daily activities. It tracks who we talk to and where we are. It will log calls, take pictures, and keep our contact list close at hand. In short it has become an indispensable piece of evidence in a criminal investigation.

Want to know where your suspect was last Saturday? The cellular service provider can provide you the location information of the cellular phone as it relates to the provider’s network. What about the last person your victim called? Both the cellular phone and the cellular provider will keep a record of this. How about finding gang member photos associated with their gang moniker? It will be located within their cellular phones.

Information relating to a cellular phone will be found in two places. In the records possessed by the cellular service provider and in the cellular device itself.

**Getting Information From The Cellular Provider**

The following is offered to provide guidance on drafting a search warrant for the production of records maintained by the cellular provider.

The first step in obtaining records from a cellular service provider is to identify the provider. A cellular phone carrier can be queried directly to ascertain if they provide service to a known number. Information on legal contacts for cellular service providers may be found at http://www.search.org/programs/hightech/isp/ The North American Numbering Plan Administration also tracks the numbers that have been assigned to service providers. (http://www.nationalnanpa.com) Since a cellular phone number may now be ported (transferred) by a consumer to another cellular service provider, law enforcement should make a number porting check. Law enforcement may sign up for the service at (http://npac.com/lawenforcement/ivr.shtml)

The second step in obtaining records from a cellular service provider is a preservation request to “freeze” stored records and communications pursuant to 18 U.S.C. § 2703(f). Many cellular service providers maintain records for only a short period of time. This request can be used as a directive to third-party providers to preserve records and not disclose the investigation to the suspect. This is an important tool to use to prevent third-party providers from writing over or deleting data you need while you obtain a warrant. Currently there are no laws which govern how long a third-party provider must retain log or other information. Sample preservation orders can be found at (Appendix C).
It is also recommended that you contact the cellular service provider to ascertain the type and nature of records kept and any special terms or definitions that the carrier uses to describe those records. Any request for records should be limited to only the records that are needed. Do not request all of the categories of records listed unless it is truly needed for your case. Cellular phone records can be described in the warrant as follows:

A.) Subscriber information

Note: This should give you the name, address, phone numbers, and other personal identifying information relating to the subscriber.

B.) Account comments

Note: Anytime the provider has contact with the customer or modifies the customer's account a notation will be made by a service representative on the account.

C.) Credit information

Note: Most providers run a credit report on customer prior to activating the account.

D.) Billing records

Note: Do not ask for toll information; that is a landline term for long distance. Specify period desired.

E.) Outbound and inbound call detail

Note: This is the real time, current activity that is not yet on the customer's bill. "Inbound" is usually available for only a limited time (45 days) which gives other cellular phones calling the target number.

F.) Call origination / termination location

Note: Available for a limited time (45 days) and gives location information on cell sites used, length of call, date, time, numbers dialed. With a GPS enabled phone it gives location of phone.

G.) Physical address of cell sites and RF coverage map

Note: Needed to determine where cell site is located when you receive inbound & outbound or call origination & termination location. The RF coverage map models the theoretical radio frequency coverage of the towers in the system. You will want to limit this request to a specified geographical area.

H.) Any other cellular telephone numbers that dial the same numbers as (xxx) xxx-xxxx
Note: If you want to know who calls the same number the target calls (for example a pager or landline number). Available for only a limited time (45 days).

I.) Subscriber information on any cellular numbers that (xxx) xxx-xxxx dials

Note: Subscriber information on the carrier’s network that is dialing the target.

J.) All of the above records whether possessed by cellular service provider [target of warrant] or any other cellular service provider

Note: If you anticipate the suspect may be roaming or if the number is roaming in the providers market, you may be able to obtain information from other cellular carriers if you include this language in your description of records.

K.) All stored communications or files, including voice mail, email, digital images, buddy lists, and any other files associated with user accounts identified as: account(s) xxxxxx, mobile numbers (xxx) xxx-xxxx, or e-mail account

Note: Cellular service providers now offer similar services to an internet service provider (ISP) and maintain the same type of records such as text messaging, e-mail, and file storage for the transfer of data including digital pictures. Limit your request to what you need.

L.) All connection logs and records of user activity for each such account including:

1. Connection dates and times.
2. Disconnect dates and times.
3. Method of connection (e.g., telnet, ftp, http)
4. Data transfer volume.
5. User name associated with the connections.
6. Telephone caller identification records.
7. Any other connection information, such as the Internet Protocol address of the source of the connection.
8. Connection information for the other computer to which the user of the above-referenced accounts connected, by any means, during the connection period, including the destination IP address, connection time and date, disconnect time and date, method of connection to the destination computer, and all other information related to the connection from cellular service provider.

Note: The above is a standard request made to ISP to track connection information. Remember with the type of cellular service offered today the user can send a message from the phone or from the associated account via a computer or other access device.

M.) Any other records or accounts, including archived records related or associated to the
above referenced names, user names, or accounts and any data field name definitions that describe these records.

Note: This is the catch all to use when you want everything. This request also includes "archived" information. Many companies now "archive" records thus allowing for the preservation of subscriber records for a significant time. Archived records are usually stored in a spreadsheet format encompassing a variety of data fields. You must request the data field name definitions in order to understand the spreadsheet.

N.) PUK for SIM card # __________

Note: Subscriber Identity Module (SIM) is a smart card inside of a GSM cellular phone that encrypts voice and data transmissions and stores data about the specific user so that the user can be identified and authenticated to the network supplying the service. The SIM also stores data such as personal phone settings specific to the user and phone numbers.

SIM cards can be password protected by the user. Even with this protection SIM cards may still be unlocked with a personal unlock key (PUK) that is available from the service provider. Note that after ten wrong PUK codes, the SIM card locks forever.

O.) All connection logs and records of user activity for the cellular tower identified as (describe cell towers location and identification #) for the time period between (list time period).

Note: Often referred to as a "tower dump," this request allows you to review all users that connect to a specific tower during a specified time frame. This search warrant of last resort is used to see if the tower data can provide possible suspects that were in the area when a crime occurred. Data from a tower may consist of a list of telephone numbers, call start times and end times.

Cellular service providers maintain the physical address of their cell sites. (See "G.") Multiple carriers may share a tower. In that each carrier maintains its own records, a search warrant would have to be served on each carrier that uses the identified tower. You will want to request that these records be produced to you in an electronic format such as excel or txt.

A search warrant for the production of records held by a cellular service provider should always include an order for non-disclosure. The cellular service provider will notify the customer of the search warrant unless there is a non-disclosure order. This order will delay notification for 90 days and can be extended for an additional 90 days. (See California Public Utilities Commission decision No. 93361 (7/21/1981).) A non-disclosure order may be phrased as follows:

ORDER FOR NON-DISCLOSURE OF SEARCH WARRANT
It is further ordered that cellular service provider not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this order for 90 days in that such a disclosure could give the subscriber an opportunity to destroy evidence, notify confederates, or flee or continue his flight from prosecution.

Now that we have listed what records we are seeking, probable cause must be shown in the affidavit for each of the listed items. The following is sample language justifying the need for the production of specified records that can be used as a starting point for drafting the search warrant affidavit:

P.) Through experience and training, your affiant knows cellular service providers maintain records related to subscriber information, account registration, credit information, billing and airtime records, outbound and inbound call detail, connection time and dates, Internet routing information (Internet Protocol numbers), and message content, that may assist in the identification of person/s accessing and utilizing the account.

Q.) Through experience and training, your affiant knows that the cellular service provider maintains records that include cell site information and GPS location. Cell site information shows which cell site a particular cellular telephone was within at the time of the cellular phone’s usage. Some model cellular phone are GPS enabled which allows the provider and user to determine the exact geographic position of the phone. Further, the cellular service provider maintains cell site maps that show the geographical location of all cell sites within its service area. Using the cell site geographical information or GPS information, officers would be able to determine the physical location of the individual using the cell phone number (xxx) xxx-xxxx, which according to corroborating sources listed above was/is in use by the suspect. That information is necessary to the investigating officers in order to ________________________________

R.) Cellular tower (describe location and tower #) is located approximately _____ from the location where John Does body was discovered. Through experience and training, your affiant knows that cell towers maintained by cellular service providers contain records that include connection logs and records of user activity that have accessed the cell tower. These records may include telephone numbers, call start times and end times. Accessing this information would enable officers to identify individuals who cellular device accessed this cellular tower during the time period of the crime. That information is necessary to identify possible witnesses and or suspects.

It is also recommended that you include within the affidavit the authority which allows a search warrant to be served by facsimile (fax) for the production of records maintained outside of California.

S.) Your affiant is aware that cellular service provider is located within the State of______. Pursuant to Penal Code section 1524.2 and Corporations Code section 2105 a California search warrant may be served upon them and they have requested that this warrant be
served by facsimile to the attention of ___________ at (xxx) xxx-xxxx.

Note: Some judges question their authority to authorize out-of-state service of the warrant. Please refer them to Corporation Code section 2105(5)(B). The term “properly served” includes delivery to a person or entity listed in Corporation Code section 2110. Corporation Code section 2110 allows service on any “natural person designated by it as agent for service of process.” The above paragraph is the corporation designating an agent for the service of process.

A word of caution. If you use the cellular subscriber records to attempt to determine the specific physical location of an individual’s position there are a couple of questions that must be answered.

First question is call overloading. When the maximum call processing capacity of a specified cell tower is reached it may be designed to hand off calls to other cell towers. Thus, a tower that the records reflect handled a call may have off-loaded the call to another cellular tower. The cellular provider will be able to check the cellular traffic on a specified cellular tower to determine whether or not any calls were off loaded.

Second question is whether the records reflecting the placement of a specified cellular tower’s directional antenna is accurate. Occasionally the cellular provider may make adjustments to the cellular towers directional antenna that is not reflected in the records. Since the physical location of an individual’s position will be based upon this directional antenna, its placement should be confirmed prior to trial.
Getting Information From The Cellular Device

The cellular device (the cell phone) is simply a container of information. The same rules for computer search warrants apply to cellular devices. For the purposes of this paper we are assuming that the affiant officer has previously legally obtained the cellular device and has already propounded appropriate language/facts within the warrant denoting that any desired digital evidence is either:

- An instrumentality of the crime investigated; or
- A storage container for illegal “contraband” such as child pornography; or
- A storage container for evidence relating to the crime such as “records,” “address books,” “call logs,” “photos,” other items that could be recovered from the cellular device.

Furthermore, for purposes of this paper, we are assuming that the cellular device will be examined by a forensic examiner. This means that the cellular device or other container containing digital media will be removed from its current location (evidence locker) for search.

The following is presented within the search warrant.

YOU ARE THEREFORE COMMANDED TO SEARCH:

One (describe cellular device), Model #______, on the ________ network with access number ________, serial number __________, and FCC ID#_________________ (the "Cell Phone").

Note: The above language assumes that you are in possession of the cellular device. When you have the device it only needs to be described with sufficient particularity that anyone would recognize it.

Located at (list current location of the device)

Note: This may be your agency

FOR THE FOLLOWING PROPERTY:

A.) Describe the records that you have probable cause to believe will be recovered from the cellular phone.

Note: Description of records must be “reasonable particular.” (Pen. Code, §§ 1525, 1529.) As opposed to trying to describe the record by its type, describe the item as it pertains to a specified person or between specified dates. For example, any and all records showing communication between suspect John Doe and any other party relating to the sale of methamphetamine occurring between July 1, 2008 and December 30, 2009.
The terms "records," "information," and "property" includes all of the foregoing items of evidence in whatever form and by whatever means that may have been created or stored, including records, whether stored on paper, on magnetic media such as tape, cassette, disk, diskette or on memory storage devices such as optical disks, programmable instruments such as telephones, electronic address books, calculators, or any other storage media, or any other form of "writing" as defined by Evidence Code section 250, together with indicia of use, ownership, possession, or control of such "records," "information," and "property".

Note: This language expands the definition of property and follows the description of specific records to be searched for and seized. Currently, the courts have been inclined to treat computers and other electronic storage devices as ordinary containers. Thus, warrants describing specified information are generally held to permit searches of containers capable of storing that information. (See New York v. Loorie (1995) 630 N.Y.S.2d 483 (finding police did not exceed scope of warrant by searching contents of computer's internal drive and external disks when warrant only authorized taking possession of property).) However, since this issue has not been directly addressed by any California court, an affiant officer should still include the above language.

Investigating officers are authorized, at their discretion, to seize all "computer systems," "computer program or software," and "supporting documentation" as defined by Penal Code section 502, subdivision (b), including any supporting hardware, software, or documentation that is necessary to the use the system or is necessary to recover digital evidence from the system and any associated peripherals that are believed to contain some or all of the evidence described in the warrant, and to conduct an offsite search of the seized items for the evidence described. Investigating officers and those agents acting under the direction of the investigating officers are authorized to access all computer data to determine if the data contains "records," "information," and "property" as described above. If necessary, investigating officers are authorized to employ the use of outside experts, acting under the direction of the investigating officers, to access and preserve computer data. The investigating officer has (insert current forensic turnaround time + 10 days) days from the date of seizure to determine if the seized computer systems and associated peripherals contain some or all of the evidence described in the warrant. 

Note: When confronted with a computer or cellular device at a search scene, searching officers have one of two choices; either search the computer at the scene or justify its removal in the search warrant for a subsequent search off scene. The above language in conjunction with the below language (E-M) is suggested to justify removing computers or cellular devices for a subsequent search off scene. (See United States v. Kuprovich (1997)
997 F. Supp. 246 (upholding warrant language authorizing removal of computer for latter search); United States v. Gawrysiak (1997) 972 F.Supp. 853.) Note that the last three sentences state that the forensic examination will be completed within a specified time period. This is in response to federal magistrate specifying short turn around times of forensic examinations. (See U.S. v. Brunnette (D. Me. 1999) 76 F.Supp. 2d 30. [suppression grated with investigator failed to comply with court ordered forensic completion date]. The time period specified will reflect the current forensic completion cycle at the issuing agency plus 10 days.

D.) "It is hereby ordered that Apple Inc. assist law enforcement agents in the search of one Apple iPhone Telephone, Model #________, on the ______ network with access number ________, serial number __________, and FCC ID#________________ (the "Cell Phone").

It is hereby further ordered that Apple shall assist law enforcement agents in searching the cell phone, assistance that shall include, but is not limited to, bypassing the Cell Phone user's passcode so that the agents may search the Cell Phone."

or

"It is hereby ordered that Google Inc. provide the username for the cellular device identified as T-Mobile HTC/G-1 Android platform cell phone, Model #________, on the ______ network with access number ________, serial number __________, and FCC ID#________________ (the "cellular device") by providing the associated user name and by resetting the cellular devices password.

It is hereby further ordered that Google shall reset the pass code for this cellular device and provide the pass code to law enforcement.

Note: Some corporations will voluntarily provide officers with technical assistance in gaining access to the devices. Although the language in "Section C" above allows "the use of outside experts" some corporations may require greater specificity.

The affidavit still is required to support the above listed requests. The following is sample language justifying the need for the removal of the item for subsequent examination and search by the forensic examiner:

Pursuant to SW #__________, which is attached and incorporated by reference (Attachment A), your affiant has been tasked to do a forensic examination of a T-Mobile HTC/G-1 Android platform cell phone.

The device is identified as T-Mobile HTC/G-1 Android platform cell phone, Model #________, on the ______ network with access number ________, serial number __________, and FCC ID#________________ (the "cellular device").
Upon examination the cellular device is locked and requires a Google/Gmail user name and password to unlock the device. At this time we do not have the technology to bypass this lock. We have been unable to download the contents of the phone onto a CellBrite, a cellular forensic tool, because the cellular device is not USB-Debugging enabled.

Your affiant has spoken to T-Mobile and Google. I am told the only way to unlock the phone is to have the Gmail user name and password, which was required when the device was setup. We obtained the user name from Google via a exigent request, but was informed that they do not have access to particular email account passwords, as they are encrypted. Google can reset the password thus allowing access.

Therefore to be able to search this cellular device we are requesting the Gmail user name associated with the cellular device and that Google resets the password and further provides the reset pass word to law enforcement.

E.) Affiant interviewed (insert law enforcement expert’s name) employed as a (agent / computer examiner) in the Sacramento Valley High Technology Crimes Task Force (SVHTC) Based upon information related to me on, I know that digital evidence can be stored on a variety of systems and storage devices including, but not limited to, Electronic data processing and storage devices, computers and computer systems including central processing units: internal and peripheral storage devices such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drive and tapes, optical storage devices or other memory storage devices: peripheral input/output devices such as keyboards, printers, video display monitors, optical readers, and related communications devices such as cellular devices and PDAs.

F.) (insert law enforcement expert’s name) informed affiant that in connection with his employment, he uses computer systems as well as conducting computer-related investigations. In the past two years, (insert law enforcement expert’s name) has supervised or participated in (insert number) executions of search warrants for digital stored records and evidence. (insert law enforcement expert’s name) informed affiant that conducting a search of a cellular device or computer storage system, documenting the search, and making evidentiary and discovery copies is a lengthy process. It is necessary to determine that no security devices are in place, which could cause the destruction of evidence during the search; in some cases it is impossible even to conduct the search without expert technical assistance. Since digital evidence is extremely vulnerable to tampering or to destruction through error, electrical outages, and other causes, removal of the system from the premises will assist in retrieving the records authorized to be seized, while avoiding accidental destruction or deliberate alteration of the records. It would be extremely difficult to secure the system on the premises during the entire period of the search.

G.) (insert law enforcement expert’s name) also stated that whether records are stored on cellular device or computer storage system, even when they purportedly have been erased or deleted, they may still be retrievable. (insert law enforcement expert”s name) is
familiar with the methods of restoring “lost” data commonly employed by computer users, and has used those methods himself. (insert law enforcement expert’s name) has also obtained the assistance of a computer expert in several cases, in order to obtain the contents of computer-stored evidence where normal methods were unsuccessful. He stated that should such data retrieval be necessary, it is time-consuming, and would add to the difficulty of securing the system on the premises during the search.

H.) (insert law enforcement expert’s name) stated that the accompanying software and docking / charging equipment must also be seized, since it would be impossible without examination to determine that it is standard, commercially available software. It is also may be necessary to have the software used to create data files and records in order to read the files and records. It is also necessary to the ability to charge the device.

I.) (insert law enforcement expert’s name) informed affiant that the system documentation, instruction manuals, and software manuals are also necessary to properly operate that specific system in order to accurately obtain and copy the records authorized to be seized.

J.) (insert law enforcement expert’s name) informed affiant that the systems pass words or keys must also be seized, since it may be impossible to access the system if it is pass word protected or other encryption devices are in place. (insert law enforcement expert’s name) informed affiant that users often record pass words or keys on material found near the computer system. These pass words or keys could be names or a combination of characters or symbols.

K.) (insert law enforcement expert’s name) informed affiant that conducting a search of a computer system, documenting the search, and making evidentiary and discovery copies for a standard computer can take over 3 business days. Complex systems or recover tasks can require an excess of 45 business days to complete. Due to the back load of computers waiting to be examined and the limited number of trained examiners (insert law enforcement expert’s name) informed affiant that the Sacramento Valley High Tech Crime Task Force is currently conducting searches of computer system within (insert current forensic turnaround time) days of receipt. (insert law enforcement expert’s name) informed affiant that the Sacramento Valley High Tech Crime Task Force would process any computer system seized pursuant to this warrant within (insert current forensic turnaround time + 10 days) days of receipt.

L.) It is respectfully requested that I be allowed to seize all original digital evidence, in whatever form it currently resides, and transport this original digital evidence to a secure Evidence Storage Facility for a proper forensic examination.

M.) Your affiant has spoken with (insert technician’s name here) and he/she has agreed to provide assistance in bypassing the pass code (encryption) and any other assistance as required to conduct a search of this device.

Note: This is only required when a corporations voluntarily provide officers with
technical assistance in gaining access to the devices and desires greater specificity then the normal order. (See Section D.)

Discovering Evidence Not Listed In Warrant During Search of a Computer or Cellular Device

If records which are not authorized to be seized, or which relate to crimes not under investigation, are discovered in the course of analysis, the searching officer must obtain supplemental warrant to expand the scope of the original search warrant. (See U.S. v. Grey (1999) 78 F.Supp.2d 524) While there is a argument that such records were lawfully discovered in “plain view,” in light of current case law it is prudent that when the records are first discovered that the search warrant be expanded to encompass them.
Search Warrant Language For Cellular Phones\(^1\) (8/10)

Cellular phones have become the virtual biographer of our daily activities. It tracks who we talk to and where we are. It will log calls, take pictures, and keep our contact list close at hand. In short it has become an indispensable piece of evidence in a criminal investigation.

Want to know where your suspect was last Saturday? The cellular service provider can provide you the location information of the cellular phone as it relates to the provider’s network. What about the last person your victim called? Both the cellular phone and the cellular provider will keep a record of this. How about finding gang member photos associated with their gang moniker? It will be located within their cellular phones.

Information relating to a cellular phone will be found in two places. In the records possessed by the cellular service provider and in the cellular device itself.

**Getting Information From The Cellular Provider**

The following is offered to provide guidance on drafting a search warrant for the production of records maintained by the cellular provider.

The first step in obtaining records from a cellular service provider is to identify the provider. A cellular phone carrier can be queried directly to ascertain if they provide service to a known number. Information on legal contacts for cellular service providers may be found at [http://www.search.org/programs/hightech/isp/](http://www.search.org/programs/hightech/isp/) The North American Numbering Plan Administration also tracks the numbers that have been assigned to service providers. ([http://www.nationalnanpa.com](http://www.nationalnanpa.com)) Since a cellular phone number may now be ported (transferred) by a consumer to another cellular service provider, law enforcement should make a number porting check. Law enforcement may sign up for the service at [http://www.nationalpooling.com/forms/law/index.htm](http://www.nationalpooling.com/forms/law/index.htm)

The second step in obtaining records from a cellular service provider is a preservation request to “freeze” stored records and communications pursuant to 18 U.S.C. § 2703(f). Many cellular service providers maintain records for only a short period of time. This request can be used as a directive to third-party providers to preserve records and not disclose the investigation to the suspect. This is an important tool to use to prevent third-party providers from writing over or deleting data you need while you obtain a warrant. Currently there are no laws which govern how long a third-party provider must retain log or other information. Sample preservation orders can be found at: [Appendix C] or
It is also recommended that you contact the cellular service provider to ascertain the type and nature of records kept and any special terms or definitions that the carrier uses to describe those records. Any request for records should be limited to only the records that are needed. Do not request all of the categories of records listed unless it is truly needed for your case. Cellular phone records can be described in the warrant as follows:

A.) Subscriber information

*Note: This should give you the name, address, phone numbers, and other personal identifying information relating to the subscriber.*

B.) Account comments

*Note: Anytime the provider has contact with the customer or modifies the customer’s account a notation will be made by a service representative on the account.*

C.) Credit information

*Note: Most providers run a credit report on customer prior to activating the account.*

D.) Billing records

*Note: Do not ask for toll information; that is a landline term for long distance. Specify period desired.*

E.) Outbound and inbound call detail

*Note: This is the real time, current activity that is not yet on the customer's bill. “Inbound” is usually available for only a limited time (45 days) which gives other cellular phones calling the target number.*

F.) Call origination / termination location

*Note: Available for a limited time (45 days) and gives location information on cell sites used, length of call, date, time, numbers dialed. With a GPS enabled phone it gives location of phone.*

G.) Physical address of cell sites and RF coverage map

*Note: Needed to determine where cell site is located when you receive inbound & outbound or call origination & termination location. The RF coverage map models the theoretical radio frequency coverage of the towers in the system. You will want to limit this request to a specified geographical area.*
H.) Any other cellular telephone numbers that dial the same numbers as (xxx) xxx-xxxx

Note: If you want to know who calls the same number the target calls (for example a pager or landline number). Available for only a limited time (45 days).

I.) Subscriber information on any cellular numbers that (xxx) xxx-xxxx dials

Note: Subscriber information on the carrier’s network that is dialing the target.

J.) All of the above records whether possessed by cellular service provider [target of warrant] or any other cellular service provider

Note: If you anticipate the suspect may be roaming or if the number is roaming in the providers market, you may be able to obtain information from other cellular carriers if you include this language in your description of records.

K.) All stored communications or files, including voice mail, email, digital images, buddy lists, and any other files associated with user accounts identified as: account(s) xxxxxxx, mobile numbers (xxx) xxx-xxxx, or e-mail account

Note: Cellular service providers now offer similar services to an internet service provider (ISP) and maintain the same type of records such as text messaging, e-mail, and file storage for the transfer of data including digital pictures. Limit your request to what you need.

L.) All connection logs and records of user activity for each such account including:

1. Connection dates and times.
2. Disconnect dates and times.
3. Method of connection (e.g., telnet, ftp, http)
4. Data transfer volume.
5. User name associated with the connections.
6. Telephone caller identification records.
7. Any other connection information, such as the Internet Protocol address of the source of the connection.
8. Connection information for the other computer to which the user of the above-referenced accounts connected, by any means, during the connection period, including the destination IP address, connection time and date, disconnect time and date, method of connection to the destination computer, and all other information related to the connection from cellular service provider.

Note: The above is a standard request made to ISP to track connection information. Remember with the type of cellular service offered today the user can send a message from the phone or from the associated account via a computer or other access device.
M.) Any other records or accounts, including archived records related or associated to the above referenced names, user names, or accounts and any data field name definitions that describe these records.

Note: This is the catch all to use when you want everything. This request also includes "archived" information. Many companies now "archive" records thus allowing for the preservation of subscriber records for a significant time. Archived records are usually stored in a spreadsheet format encompassing a variety of data fields. You must request the data field name definitions in order to understand the spreadsheet.

N.) PUK for SIM card # _________

Note: Subscriber Identity Module (SIM) is a smart card inside of a GSM cellular phone that encrypts voice and data transmissions and stores data about the specific User so that the User can be identified and authenticated to the network supplying the service. The SIM also stores data such as personal phone settings specific to the User and phone numbers.

SIM cards can be password protected by the User. Even with this protection SIM cards may still be unlocked with a personal unlock key (PUK) that is available from the service provider. Note that after ten wrong PUK codes, the SIM card locks forever.

O.) All connection logs and records of user activity for the cellular tower identified as (describe cell towers location and identification #) for the time period between (list time period).

Note: Often referred to as a "tower dump," this request allows you to review all Users that connect to a specific tower during a specified time frame. This search warrant of last resort is used to see if the tower data can provide possible suspects that were in the area when a crime occurred. Data from a tower may consist of a list of telephone numbers, call start times and end times.

Cellular service providers maintain the physical address of their cell sites. (See "G.") Multiple carriers may share a tower. In that each carrier maintains its own records, a search warrant would have to be served on each carrier that uses the identified tower. You will want to request that these records be produced to you in an electronic format such as excel or txt.

A search warrant for the production of records held by a cellular service provider should always include an order for non-disclosure. The cellular service provider will notify the customer of the search warrant unless there is a non-disclosure order. This order will delay notification for 90 days and can be extended for an additional 90 days. (See California Public Utilities Commission decision No. 93361 (7/21/1981).) A non-disclosure order may be phrased as follows:

ORDER FOR NON-DISCLOSURE OF SEARCH WARRANT
It is further ordered that cellular service provider not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this order for 90 days in that such a disclosure could give the subscriber an opportunity to destroy evidence, notify confederates, or flee or continue his flight from prosecution.

Now that we have listed what records we are seeking, probable cause must be shown in the affidavit for each of the listed items. The following is sample language justifying the need for the production of specified records that can be used as a starting point for drafting the search warrant affidavit:

**P.)** Through experience and training, your affiant knows cellular service providers maintain records related to subscriber information, account registration, credit information, billing and airtime records, outbound and inbound call detail, connection time and dates, Internet routing information (Internet Protocol numbers), and message content, that may assist in the identification of person/s accessing and utilizing the account.

**Q.)** Through experience and training, your affiant knows that the cellular service provider maintains records that include cell site information and GPS location. Cell site information shows which cell site a particular cellular telephone was within at the time of the cellular phone’s usage. Some model cellular phones are GPS enabled which allows the provider and user to determine the exact geographic position of the phone. Further, the cellular service provider maintains cell site maps that show the geographical location of all cell sites within its service area. Using the cell site geographical information or GPS information, officers would be able to determine the physical location of the individual using the cell phone number (xxx) xxx-xxxx, which according to corroborating sources listed above was/is in use by the suspect. That information is necessary to the investigating officers in order to ___________________________

**R.)** Cellular tower (describe location and tower #) is located approximately _____ from the location where John Does body was discovered. Through experience and training, your affiant knows that cell sites maintained by cellular service providers contain records that include connection logs and records of user activity that have accessed the cell tower. These records may include telephone numbers, call start times and end times. Accessing this information would enable officers to identify individuals who cellular device accessed this cellular tower during the time period of the crime. That information is necessary to identify possible witnesses and or suspects.

It is also recommended that you include within the affidavit the authority which allows a search warrant to be served by facsimile (fax) for the production of records maintained outside of California.

**S.)** Your affiant is aware that cellular service provider is located within the State of _______. Pursuant to Penal Code section 1524.2 and Corporations Code section 2105 a California
search warrant may be served upon them and they have requested that this warrant be served by facsimile to the attention of ____________ at (xxx) xxx-xxxx.

Note: Some judges question their authority to authorize out-of-state service of the warrant. Please refer them to Corporation Code section 2105(5)(B). The term "properly served" includes delivery to a person or entity listed in Corporation Code section 2110. Corporation Code section 2110 allows service on any "natural person designated by it as agent for service of process." The above paragraph is the corporation designating an agent for the service of process.

A word of caution. If you use the cellular subscriber records to attempt to determine the specific physical location of an individual’s position there are a couple of questions that must be answered.

First question is call overloading. When the maximum call processing capacity of a specified cell tower is reached it may be designed to hand off calls to other cell towers. Thus, a tower that the records reflect handled a call may have off-loaded the call to another cellular tower. The cellular provider will be able to check the cellular traffic on a specified cellular tower to determine whether or not any calls were off loaded.

Second question is whether the records reflecting the placement of a specified cellular tower’s directional antenna is accurate. Occasionally the cellular provider may make adjustments to the cellular towers directional antenna that is not reflected in the records. Since the physical location of an individual’s position will be based upon this directional antenna, its placement should be confirmed prior to trial.
Getting Information From The Cellular Device

The cellular device (the cell phone) is simply a container of information. The same rules for computer search warrants apply to cellular devices. For the purposes of this paper we are assuming that the affiant officer has previously legally obtained the cellular device and has already propounded appropriate language/facts within the warrant denoting that any desired digital evidence is either:

- An instrumentality of the crime investigated; or
- A storage container for illegal “contraband” such as child pornography; or
- A storage container for evidence relating to the crime such as “records,” “address books,” “call logs,” “photos,” other items that could be recovered from the cellular device.

Furthermore, for purposes of this paper, we are assuming that the cellular device will be examined by a forensic examiner. This means that the cellular device or other container containing digital media will be removed from its current location (evidence locker) for search.

The following is presented within the search warrant.

YOU ARE THEREFORE COMMANDED TO SEARCH:

One (describe cellular device), Model #______, on the ______ network with access number ___________, serial number __________, and FCC ID#_____________ (the "Cell Phone").

Note: The above language assumes that you are in possession of the cellular device. When you have the device it only needs to be described with sufficient particularity that anyone would recognize it.

Located at (list current location of the device)

Note: This may be your agency

FOR THE FOLLOWING PROPERTY:

A.) Describe the records that you have probable cause to believe will be recovered from the cellular phone.

Note: Description of records must be “reasonable particular.” (Pen. Code, §§ 1525, 1529.) As opposed to trying to describe the record by its type, describe the item as it pertains to a specified person or between specified dates. For example, any and all records showing communication between suspect John Doe and any other party relating to the sale of methamphetamine occurring between July 1, 2008 and December 30, 2009.
B.) The terms “records,” “information,” and “property” includes all of the foregoing items of evidence in whatever form and by whatever means that may have been created or stored, including records, whether stored on paper, on magnetic media such as tape, cassette, disk, diskette or on memory storage devices such as optical disks, programmable instruments such as telephones, electronic address books, calculators, or any other storage media, or any other form of “writing” as defined by Evidence Code section 250, together with indicia of use, ownership, possession, or control of such “records,” “information,” and “property”.

Note: This language expands the definition of property and follows the description of specific records to be searched for and seized. Currently, the courts have been inclined to treat computers and other electronic storage devices as ordinary containers. Thus, warrants describing specified information are generally held to permit searches of containers capable of storing that information. (See New York v. Loorie (1995) 630 N.Y.S.2d 483 (finding police did not exceed scope of warrant by searching contents of computer’s internal drive and external disks when warrant only authorized taking possession of property).) However, since this issue has not been directly addressed by any California court, an affiant officer should still include the above language.

C.) Investigating officers are authorized, at their discretion, to seize all “computer systems,” “computer program or software,” and “supporting documentation” as defined by Penal Code section 502, subdivision (b), including any supporting hardware, software, or documentation that is necessary to the use the system or is necessary to recover digital evidence from the system and any associated peripherals that are believed to contain some or all of the evidence described in the warrant, and to conduct an offsite search of the seized items for the evidence described. Investigating officers and those agents acting under the direction of the investigating officers are authorized to access all computer data to determine if the data contains “records,” “information,” and “property” as described above. If necessary, investigating officers are authorized to employ the use of outside experts, acting under the direction of the investigating officers, to access and preserve computer data. The investigating officer has (insert current forensic turnaround time + 10 days) days from the date of seizure to determine if the seized computer systems and associated peripherals contain some or all of the evidence described in the warrant. [or you may want to consider the following: Any digital evidence found during the execution of this search warrant will be seized, transported from the scene, and analyzed in a reasonably prudent time.] If no evidence of criminal activity is discovered relating to the seized computer systems and associated peripherals, the system will be returned promptly.

Note: When confronted with a computer or cellular device at a search scene, searching officers have one of two choices; either search the computer at the scene or justify its removal in the search warrant for a subsequent search off scene. The above language in conjunction with the below language (E-M) is suggested to justify removing computers or cellular devices for a subsequent search off scene. (See United States v. Kusrovi (1997)
997 F. Supp. 246 [upholding warrant language authorizing removal of computer for latter search]; United States v. Gawrysiak (1997) 972 F.Supp. 853.) Note that the last three sentences state that the forensic examination will be completed within a specified time period. This is in response to federal magistrate specifying short turn around times of forensic examinations. (See U.S. v. Brunnette (D. Me. 1999) 76 F.Supp.2d 30. [suppression grated with investigator failed to comply with court ordered forensic completion date]. The time period specified will reflect the current forensic completion cycle at the issuing agency plus 10 days.

D.) "It is hereby ordered that Apple Inc. assist law enforcement agents in the search of one Apple iPhone Telephone, Model #______, on the _______ network with access number ________, serial number __________, and FCC ID#__________________ (the "Cell Phone").

It is hereby further ordered that Apple shall assist law enforcement agents in searching the cell phone, assistance that shall include, but is not limited to, bypassing the Cell Phone user's passcode so that the agents may search the Cell Phone."

or

"It is hereby ordered that Google Inc. provide the username for the cellular device identified as T-Mobile HTC/G-1 Android platform cell phone, Model #______, on the _______ network with access number ________, serial number __________, and FCC ID#__________________ (the "cellular device") by providing the associated user name and by resetting the cellular devices password.

It is hereby further ordered that Google shall reset the pass code for this cellular device and provide the pass code to law enforcement.

Note: Some corporations will voluntarily provide officers with technical assistance in gaining access to the devices. Although the language in "Section C" above allows "the use of outside experts" some corporations may require greater specificity.

The affidavit still is required to support the above listed requests. The following is sample language justifying the need for the removal of the item for subsequent examination and search by the forensic examiner:

Pursuant to SW #__________, which is attached and incorporated by reference (Attachment A), your affiant has been tasked to do a forensic examination of a T-Mobile HTC/G-1 Android platform cell phone.

The device is identified as T-Mobile HTC/G-1 Android platform cell phone, Model #______, on the _______ network with access number ________, serial number __________, and FCC ID#__________________ (the "cellular device").
Upon examination the cellular device is locked and requires a Google/Gmail user name and password to unlock the device. At this time we do not have the technology to bypass this lock. We have been unable to download the contents of the phone onto a CellBrite, a cellular forensic tool, because the cellular device is not USB-Debugging enabled.

Your affiant has have spoken to T-Mobile and Google. I am told the only way to unlock the phone is to have the Gmail user name and password, which was required when the device was setup. We obtained the user name from Google via a exigent request, but was informed that they do not have access to particular email account passwords, as they are encrypted. Google can reset the password thus allowing access.

Therefore to be able to search this cellular device we are requesting the Gmail user name associated with the cellular device and that Google resets the password and further provides the reset pass word to law enforcement.

E.) Affiant interviewed (insert law enforcement expert’s name) employed as a (agent / computer examiner) in the Sacramento Valley High Technology Crimes Task Force (SVHTC) Based upon information related to me,

I know that digital evidence can be stored on a variety of systems and storage devices including, but not limited to, Electronic data processing and storage devices, computers and computer systems including central processing units: internal and peripheral storage devices such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drive and tapes, optical storage devices or other memory storage devices: peripheral input/output devices such as keyboards, printers, video display monitors, optical readers, and related communications devices such as cellular devices and PDAs.

F.) (insert law enforcement expert’s name) informed affiant that in connection with his employment, he uses computer systems as well as conducting computer-related investigations. In the past two years, (insert law enforcement expert’s name) has supervised or participated in (insert number) executions of search warrants for digital stored records and evidence. (insert law enforcement expert’s name) informed affiant that conducting a search of a cellular device or computer storage system, documenting the search, and making evidentiary and discovery copies is a lengthy process. It is necessary to determine that no security devices are in place, which could cause the destruction of evidence during the search; in some cases it is impossible even to conduct the search without expert technical assistance. Since digital evidence is extremely vulnerable to tampering or to destruction through error, electrical outages, and other causes, removal of the system from the premises will assist in retrieving the records authorized to be seized, while avoiding accidental destruction or deliberate alteration of the records. It would be extremely difficult to secure the system on the premises during the entire period of the search.

G.) (insert law enforcement expert’s name) also stated that whether records are stored on cellular device or computer storage system, even when they purportedly have been erased or deleted, they may still be retrievable. (insert law enforcement expert”s name) is
familiar with the methods of restoring “lost” data commonly employed by computer
users, and has used those methods himself. (insert law enforcement expert’s name) has
also obtained the assistance of a computer expert in several cases, in order to obtain the
contents of computer-stored evidence where normal methods were unsuccessful. He
stated that should such data retrieval be necessary, it is time-consuming, and would add
to the difficulty of securing the system on the premises during the search.

H.) (insert law enforcement expert’s name) stated that the accompanying software and
docking / charging equipment must also be seized, since it would be impossible without
examination to determine that it is standard, commercially available software. It is also
may be necessary to have the software used to create data files and records in order to
read the files and records. It is also necessary to the ability to charge the device.

I.) (insert law enforcement expert’s name) informed affiant that the system documentation,
instruction manuals, and software manuals are also necessary to properly operate that
specific system in order to accurately obtain and copy the records authorized to be seized.

J.) (insert law enforcement expert’s name) informed affiant that the systems pass words or
keys must also be seized, since it may be impossible to access the system if it is pass
word protected or other encryption devices are in place. (insert law enforcement expert’s
name) informed affiant that users often record pass words or keys on material found near
the computer system. These pass words or keys could be names or a combination of
characters or symbols.

K.) (insert law enforcement expert’s name) informed affiant that conducting a search of a
computer system, documenting the search, and making evidentiary and discovery copies
for a standard computer can take over 3 business days. Complex systems or recover tasks
can require an excess of 45 business days to complete. Due to the back load of
computers waiting to be examined and the limited number of trained examiners (insert
law enforcement expert’s name) informed affiant that the Sacramento Valley High Tech
Crime Task Force is currently conducting searches of computer system within (insert
current forensic turnaround time) days of receipt. (insert law enforcement expert’s name)
informed affiant that the Sacramento Valley High Tech Crime Task Force would process
any computer system seized pursuant to this warrant within (insert current forensic
turnaround time + 10 days) days of receipt.

L.) It is respectfully requested that I be allowed to seize all original digital evidence, in
whatever form it currently resides, and transport this original digital evidence to a secure
Evidence Storage Facility for a proper forensic examination.

M.) Your affiant has spoken with (insert technician’s name here) and he/she has agreed to
provide assistance in bypassing the pass code (encryption) and any other assistance as
required to conduct a search of this device.

Note: This is only required when a corporations voluntarily provide officers with
technical assistance in gaining access to the devices and desires greater specificity than the normal order. (See Section D.)

Discovering Evidence Not Listed In Warrant During Search of a Computer or Cellular Device

If records which are not authorized to be seized, or which relate to crimes not under investigation, are discovered in the course of analysis, the searching officer must obtain supplemental warrant to expand the scope of the original search warrant. (See U.S. v. Grey (1999) 78 F.Supp.2d 524) While there is a argument that such records were lawfully discovered in “plain view,” in light of current case law it is prudent that when the records are first discovered that the search warrant be expanded to encompass them.
IS IT REAL OR MEMOREX?

IS IT REAL OR MEMOREX?

CA PENAL CODE 637.7

SURVEILLANCE TOOLS

PHOTOGRAPHY & VIDEOGRAPHY
AUDIO RECORDING (WIRES & BUGS)
TRACKING DEVICES & TECHNIQUES
THERMAL IMAGING
AERIAL SURVEILLANCE
SNEAK & PEEK SEARCH WARRANTS
CUSTODIAL MONITORING
ELECTRONIC INTERCEPTS (WIRETAPS)
COMPUTERS & THE INTERNET
PROTECTING YOUR TOOLS & TECHNIQUES

EXPECTATION OF PRIVACY

IS IT REAL OR MEMOREX?

PERCEPTIONS MATTER

BATTERIES FAIL
EQUIPMENT BREAKS
OPERATORS SCREW UP
ANALOG EVIDENCE LOST OR DAMAGED
DIGITAL EVIDENCE IS CORRUPTED
DIGITAL EVIDENCE ERASED/MISPLACED
PROBLEMS WITH AUTHENTICATION
EXPECTATION OF PRIVACY

FOURTH AMENDMENT
UNITED STATES CONSTITUTION

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

SURVEILLANCE TOOLS

□ ENHANCING YOUR SENSES
□ PHOTOGRAPHY & VIDEOGRAPHY
□ AUDIO RECORDING (WIRES & BUGS)
□ TRACKING DEVICES & TECHNIQUES
□ THERMAL IMAGING, X-RAYS, ETC.
□ AERIAL SURVEILLANCE
□ SNEAK & PEEK SEARCH WARRANTS
□ CUSTODIAL MONITORING
□ ELECTRONIC INTERCEPTS (WIRED/TAPE)
□ COMPUTERS & THE INTERNET
□Protecting your tools & techniques

ENHANCING YOUR SENSES

□ SIGHT
  ▪ BINOCULARS, TELESCOPES
  ▪ NIGHT VISION EQUIPMENT
  ▪ FLASHLIGHTS
  ▪ INFRARED & THERMAL,
  ▪ WHAT ELSE?
□ HEARING
  ▪ SHOTGUN & DISH MICROPHONES
  ▪ SPIKE MICROPHONES, LASER DEVICES
□ SMELL
  ▪ DOGS
  ▪ "SNIFTERS" OF OBJECTS OKAY GENERALLY
  ▪ "SNIFTERS" OF PEOPLE MAY REQUIRE PC
□ TRACKING OF HUMANS OKAY IF TRAINING MET

PHOTOGRAPHY & VIDEO

□ TARGET IN A PUBLIC AREA
  ▪ ROLLING SURVEILLANCE PHOTO & VIDEO
  ▪ POLE CAMERAS – CONCEALED "HIDES"
  ▪ PUBLIC SECURITY SURVEILLANCE
□ PRIVATE SECURITY SURVEILLANCE
□ NO EXPECTATION OF PRIVACY
□ BUT NO DETECTIONS FOR THE PHOTOGRAPHY

PHOTOGRAPHY & VIDEO

□ TARGET IN A PRIVATE AREA
  ▪ BEWARE REASONABLE EXPECTATION OF PRIVACY
□ UNDERCOVER PHOTOGRAPHY OR VIDEO OK
□ OFFICER OR INFORMANT PRESENT
□ PEERING THROUGH RESIDENTIAL WINDOWS
□ CONCEALED STILL OR VIDEO CAMERAS
□ GET A SEARCH WARRANT - AUDIO EXCLUDED
□ BEWARE "TWO-WAY MIRRORS"
  ▪ CAR PC 0899[c]s
  ▪ MINDREADER – bathrooms, showers,
  ▪ locker rooms, motel and hotel rooms. Warrant?
□ PENAL INSTITUTIONS EXEMPT FROM STATUTE
AUDIO RECORDING
- CA PENAL CODE 630 – 632.7
- INVASION OF PRIVACY
- EAVESDROPPING ON CONVERSATIONS
- 631 PC FELONY WOBBLER – WIRETAPS
  - CONNECTION PHYSICALLY, ELECTROCALLY, ACOUSTICALLY, BY INDUCTION, OR OTHERWISE
- 632 PC FELONY WOBBLER
  - ELECTRONICALLY AMPLIFIED OR RECORDS
  - PHYSICAL CONVERSATIONS BY TELEPHONE
  - RADIO EXCLUDED
  - PUBLIC GATHERING MAY BE EXCLUDED

AUDIO RECORDING
- 633 PC LAW ENFORCEMENT EXCEPTION
  - ATTORNEY GENERAL
  - DISTRICT ATTORNEY
  - CALIFORNIA HIGHWAY PATROL
  - POLICE CHIEF
  - SHERIFF
  - PERSON ACTING AT LAW ENFORCEMENT DIRECTION
- DOES NOT APPLY TO WIRETAPS!
- 624 PC FELONY WOBBLER
  - TRESPASSING FOR INVASION PROHIBITED
  - SEARCH WARRANT?

TRACKING DEVICES
- PUBLIC ROUTES & AREAS
- PRIVATE RESIDENCES & AREAS
  - SHUTTING OFF SENDING DEVICE
  - SHUTTING OFF RECEIVER
  - SEARCH WARRANT
- EXPECTATION OF PRIVACY

AUDIO RECORDING
- 632.5 PC FELONY WOBBLER
  - CELLULAR TELEPHONES
- 632.6 PC FELONY WOBBLER
  - CORDLESS TELEPHONES
- 642.7 PC FELONY WOBBLER
  - INTERCEPTS & RECORDS
  - LANDLINE, CELLULAR CORDLESS TELEPHONES

AUDIO RECORDING
- UNDERCOVER WIRES
  - WORN BY U/C OR INFORMANTS
  - GENERAL RULE = NO SEARCH
- HIDDEN RECORDING DEVICES – “BUGS”
  - PERMITTED IN FEDERAL INVESTIGATIONS
  - BANNED FOR CALIFORNIA LAW ENFORCEMENT
- BACK OF THE POLICE CAR
- PUBLIC PLACE?

TRACKING DEVICES
- VEHICLES & AIRCRAFT
  - INSTALLING ON EXTERNAL FRAME
  - INSTALLING INSIDE VEHICLE
  - HOOKING UP TO VEHICLE BATTERY
  - WHERE IS VEHICLE DURING INSTALLATION?
  - LOANING TRACKED VEHICLE
  - LOSING TRACKING DEVICE - THEFT & DESTRUCTION
TRACKING DEVICES
- PACKAGES
  - TRACKER
  - BEEPER ALERT
- STOLEN PROPERTY
- KNOWN CONTRABAND

AERIAL SURVEILLANCE
- OVERFLIGHTS OKAY GENERALLY
- "LEGALLY NAVIGABLE AIRSPACE"
- PHOTOGRAPHY & VIDEO OKAY
- OBSERVATIONS WITH NAKED EYE
- ENHANCED SENSES PROBABLY OKAY
  - TELESCOPES, BINOCULARS, ARTIFICIAL LIGHT
  - NIGHT VISION PROBABLY OKAY
  - NON-SENSORY ENHANCEMENT REQUIRES WARRANT

HIGH TECHNOLOGY
- THERMAL IMAGING (FLIR) = SEARCH!
- INADVERTENT THERMAL IMAGING?
- SEARCH WARRANT BASED ON PC
- "BUSTER" RADIOLOGICAL DENSITOMETER
- HIGH ENERGY SENSORS

SNEAK & PEEK WARRANTS
- JUSTIFY REASONS - GOOD CAUSE
  - ONGOING INVESTIGATION
  - LARGER CONSPIRACY
  - SAFETY OF OFFICERS OR INFORMANTS
- SURREPTITIOUS ENTRY
- NO KNOCK-NOTICE (NOBODY IS HOME!)
- OFTEN AT NIGHT - GOOD CAUSE
- DELAYED NOTICE & EXTENSIONS
- SEIZE NOTHING
- NOTE - PHOTOGRAPH - COPY - RECORD

ANTICIPATORY WARRANTS
- CONDITIONAL WARRANTS LEGAL
- DEPEND ON A TRIGGERING EVENT
- "FAIR PROBABILITY" EVIDENCE WILL BE FOUND AT A PARTICULAR PLACE... AND
- PROBABLE CAUSE TO BELIEVE TRIGGERING EVENT WILL ACTUALLY OCCUR
- DECLARE CONDITION ON WARRANT'S FACE
- USE OF TRACKERS - ALERTING DEVICES

PEN REGISTERS
- EXPECTATION OF PRIVACY
- PEN REGISTERS - #5 DIALED OUT
- TRAP & TRACE - #5 FROM CALLERS
- NOT WIRETAPS - NO CONTENT
- COURT ORDERS or SEARCH WARRANT?
- 18 USC 3121 - 3127 COURT ORDER OK
  - "Relevant to an ongoing criminal investigation."
  - Federal Court MUST issue the order
- CA ATTY GENERAL OPINION 03-406
- COURT ORDER or SEARCH WARRANT?
ELECTRONIC INTERCEPTS
aka WIRETAPS

FEDERAL vs STATE WIRES - PRACTICALITY
CA PC 639.50 et seq.
INTERCEPTION OF WIRE, TELEPHONE, ELECTRONIC DIGITAL PAGER, ELECTRONIC CELLULAR PHONE

PROBABLE CAUSE
CRIMES HAVE BEEN, ARE, OR ABOUT TO BE COMMITTED
WIRE COMMUNICATION UTILIZED TO FACILITATE CONNECT PHONES TO TARGETS
EXHAUSTION OF NORMAL INVESTIGATIVE TECHNIQUES - NECESSITY OF WIRETAP
NORMAL TECHNIQUES TRIED & FAILED
NORMAL TECHNIQUES LIKELY TO FAIL
NECESSITY - ONLY WAY TO GET INCriminating EVIDENCE

QUALIFYING CRIMES
IMPORTATION, POSSESSION FOR SALE, SALE, TRANSPORTATION, MANUFACTURE OF HEROIN, COCAINE, METHAMPHETAMINE, PCP, OVER 10 GALLONS OR 2 POUNDS.
MURDER AND SOLICITATION FOR MURDER
BOMBING OF PUBLIC OR PRIVATE PROPERTY
GANG CRIMES 186.22 PC
AGGRAVATED KIDNAPPING
WEAPONS OF MASS DESTRUCTION
CRIMES INVOLVING CERTAIN BIOLOGICAL AGENTS
CONSPIRACY FOR ANY OF THE ABOVE

OPERATORS MUST BE SPECIALLY TRAINED
IDENTIFY PHONES & CONFEDEKATES
COVERT ENTRY UNLAWFUL
GET SEARCH WARRANT IF ENTRY REQUIRED
MUST LISTEN LIVE TO STATE WIRE
STOP LISTENING IF NO CRIMINAL TALK
OVERHEAR NON-QUAlJF1ED CRimes
MUST NOTICE
90 DAYS OF WIRE'S TERMINATION OR DENIAL
10 DAYS TO DEFENDANT BEFORE TRIAL OR PRELIM

PROTECTING YOUR TOOLS
CA EVIDENCE CODE 1040, 1041, 1043
"OFFICIAL INFORMATION" means information acquired in confidence by a public employee in the course of his or her duty and not open or officially disclosed, to the public prior to the time the claim of privilege is made.
A public entity has a privilege to refuse to disclose official information unless disclosure of the information is against the public interest because there is a necessity for preserving the confidentiality of the information that outweighs the necessity for disclosure in the interests of justice.
PROTECTING TOOLS & TECHNIQUES
PROTECTING LOCATIONS
Jeffrey M. Ferguson is Senior Deputy District Attorney with the Orange County (CA) Office of District Attorney. A 27-year veteran trial prosecutor, he served fourteen years with the Narcotics Enforcement Team and is now assigned to the Felony Strike Team.

He is Deputy Director for the National Security Executive (NSX), an intelligence and policy analysis "think tank" on terrorism, transnational crime, and strategic studies.

He also served as OCDA liaison for the California Department of Justice "California Anti-Terrorism Information Center" (CATIC).

In 1990 he led the federally-funded Probation Offender Search and Seizure Enforcement (POSSE) task force, of thirty separate state and local police agencies. The program's spectacular success was praised before the United States Congress by the Office of President of the United States.

From 1994-1998 he was the Major Narcotics Vendor Program (MNVP) prosecutor, handling multi-kilo drug cases, complex conspiracies, and clandestine methamphetamine lab cases exclusively. He was also lead prosecutor for OPERATION BUYER BEWARE, an undercover clandestine methamphetamine lab penetration task force consisting of more than twenty state and local law enforcement agencies that arrested and prosecuted over 65 criminals from San Diego to Fresno. Police seized almost two hundred pounds of methamphetamine and shut down more than two dozen high-producing labs.

In 1998 he joined OPERATION ORION, targeting street gang-related narcotics trafficking, gun-running and car theft rings. Spearheaded by the Santa Ana Police Department, it included agents from the California Department of Justice and the Federal Bureau of Investigation. Ferguson personally indicted 128 criminal street gang members. Of those police located and arrested 112. More than one hundred of those went to state prison.

In 2000 he became prosecutor for OPERATION GEMINI, a deep penetration investigation of the VAGOS outlaw motorcycle gang in three states: California, Nevada, and Hawaii. He was the first prosecutor in California to convict an outlaw motorcycle gang member under California's "Street Terrorism Act."

He has received several commendations from the U.S. Drug Enforcement Administration, the California Department of Justice, the International Narcotics Enforcement Officers Association, and the Orange County Narcotic Officers Association.

Ferguson holds a Bachelor of Science degree in biology and a Bachelor of Arts degree in social ecology, both from the University of California at Irvine. He obtained his Doctorate degree in law from Western State University College of Law in Fullerton.
Specialized Surveillance, Equipment and Techniques
Specialized Surveillance, Equipment and Techniques

Robert J. Saria
Attorney at Law
jsaria@jsariaattomeys.net
Intercepted Communications

- Wiretaps
- Pager Intercepts
- Caller ID/Digital Telephones
- Answering Machines
- Voice Mail Systems
- Pen Registers
- Custodial Interceptions
- Undercover Officers and Agents

Surveillance Techniques

- Photographic
  and Video
- Stationary
  Cameras
- Tracking
  Devices
- Thermal
  Imaging
- Sneak & Peek
  Warrants

Communication Intercepts
Wire Intercept Statute

- Penal Code § 629.50
  The interception of a wire, electronic digital pager, or electronic cellular telephone communication shall only be made by Court Order pursuant to this statute.

Wire Intercepts

- "Electronic Digital Pager Communications" means any tone or digital display or tone and voice pager communication.
- "Electronic Cellular Telephone Communication" means any cellular or wireless radio telephone communication.

Qualifying Crimes

- Importation, possession for sale, transportation, manufacture or sale of 11351, 11351.5, 11352, 11375, 11375.5, 11376, 11376.5 or 1379.8 for heroin, cocaine, PCP, meth, or analogs when 10 galls or 3 lbs;
- Murder or solicitation to commit murder;
- Bombing of public or private property;
- Aggravated Kidnapping;
- Conspiracy;
- Step Act Crimes (Prop 21)
Illegal Intercepts

Any person who uses, uses, directs, or permits to use any device, including electronic devices, to intercept or access any telephone or telecommunication system or device, or any device that is connected to, or otherwise interfaces with, any telephone or telecommunication system or device, whether or not the conversation is in progress, shall be guilty of a... damages & fees.

Prop 21 Amendments

- Mobile Telephone Use
- Coverage of Interception
- Permits
- Intercepts from telephone conversations that originate from the county identified in the order

Statutory Prohibitions

- Prohibition of covert entry
- Exclusionary Rule
  - Statements
  - Evidence derived thereof
- Third Party Intercepts
- Impeachment Evidence

Specialized Surveillance and Techniques
Pagers

- General Rule
  - Interception required
  - Intercept order
- Broadcast
  - Pagers
  - Transmit neither communication nor information

Answering Machine

- Expectation of Privacy
- Probable Cause Standard
- Search Warrant

Specialized Surveillance and Techniques
Voice Mail Systems

- Subject to Wire Intercept Statutes
- Third Party Retrieval

Pen Registers/DNR

- Expectation of Privacy
- Search Warrant or Court Order

Off-the-Shelf Products

This unit records both sides of all conversations, day or night. It has a 30-second recall feature to hear any conversation you may have missed. It is powered by a 12V DC battery and has a built-in microphone. The unit comes with two dialers, one for incoming calls and one for outgoing calls. It is sold at $150.00

Specialized Surveillance and Techniques
Pen Register Data

Secure Internet/WWW
- Expectation of Privacy
- Secure Web Sites
- Subscriber Information

Specialized Surveillance and Techniques
Custodial Situations

Expectation of Privacy

As a general rule, the recognition of privacy rights for prisoners in their individual cells simply cannot be reconciled with the concept of incarceration and the needs and objectives of penal institutions. *Harper v. Prisoner* (1981) AB T.Q. 217, 633.

Custodial Situations

- Individual Cells
- Police Vehicles
- Jail Areas
  - General Rules
  - Physical Control
  - Limits
  - Brother & Sister
  - Codefendants
  - Husband & Wife

Specialized Surveillance and Techniques

- 3784 -
Creating an Expectation of Privacy

- North v. Superior Court

Private conversations between spouses in police department office without police present

Custodial Mail Intercepts

- Evidence
  - Identity
  - Intent
  - Continuing Conspiracy

- Rule
  Most policy and procedures established for the purpose of preserving jail security, to include the monitoring of mail must yield to the Fourth Amendment reasonable expectation of privacy. People v. McCawlin (1965) 170 Cal.App.3d 1, 7.

Expectation of Privacy?

Specialized Surveillance and Techniques
Eavesdropping of Communications

Electronic "Bugging"

- No authorizing statute under California Law
- Federal Law permits the use of "bugs" for purpose of surveillance
What bad guys can buy.

Off-the-Shelf Products

Penal Code §§ 630 et seq.

Invasion of Privacy Act
Penal Code § 632

"Every person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication, whether the communication is carried on among the parties or by means of a telegraph, telephone, or other device, except a radio..."

[Webster]

Penal Code § 632

Confidential Communication
- Any communication carried on in circumstances as may reasonably indicate that any person to the communication desires it to be confined to the parties hereof... excluding communications in public legislative, judicial, executive or administrative proceedings... or other circumstances which may lead parties to reasonably expect to be overheard...

Actions Barred
- Taping of Conversations
- Note taking
- Videotaping of Conversations
- Use of a Telephone
- Extension is NOT included
Law Enforcement Exception
- Limited to Scopes of Employment
  - Attorney
  - General
  - District
  - Attorney
  - Investigator
  - Sheriff
  - Chief
  - Police
  - Sheriff

Other Exceptions
- Public Utilities
- Tariffs
- Communication is exclusively within a state, county, city and county or city correctional facility
Surveillance Techniques

Fourth Amendment Analysis
- Does the target have an honest subjective expectation of privacy?
- Is this expectation of privacy objectively reasonable?

Stationary/Pole Cameras
- Public Area
- Private Area
- Enhanced Physical Abilities
  - Stealth
  - Artificial Lighting
  - Ultraviolet Light
  - Sophisticated Equipment
New Technology

- Facial Recognition Software

Sophisticated Surveillance

www.mapquest.com

Specialized Surveillance and Techniques
Governmental Privilege for "Official Information"

- Evidence Code § 1040
  - "Official Information" means information acquired in confidence by a public employee in the course of his or her duties and not used, or officially disclosed, to the public prior to the time the claim of privilege is made.
  - Disclosure is against the public interest because there is a necessity for preserving the confidentiality of the information that outweighs the necessity for disclosure in the interest of justice.
Tracking Devices

- Constitutional Limitations
- Public Roadways
- Government Property
- Stolen Property

GPS Tracking Systems

GPS-5 $1,399.99
Real time tracking system with modem
To send item location information
Thermal Imaging

- Expectation of Privacy
- Probable Cause Standard

Sneak & Peek Search Warrants

- A search warrant authorizing the entry into a protected area for the purpose of inspecting and recording the contents of the area.
**Sneak & Peek Warrants — How Different.**

- Knock-Notice
- Cover or Surrpeptitious Entry
- Permit Recordation Without Leaving a Receipt

<table>
<thead>
<tr>
<th>Affidavit Requirements</th>
<th>Statement of Probable Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need for Cover Entry</td>
<td>Results Remedy</td>
</tr>
<tr>
<td>Nighttime Service</td>
<td>Justification for Delay Notice and Extension</td>
</tr>
</tbody>
</table>

For Future Assistance

Robert J. Sene
501 S. Sutter & Sene
(916) 447-2070
RJSene@sbcglobal.net
SAN DIEGO COUNTY DISTRICT ATTORNEY

PROTOCOL FOR PRESERVING DIGITAL MEDIA

The San Diego District Attorney’s Legal Policy Committee has considered the impact of digital media issues and has adopted the following protocol.

PROTOCOL FOR PRESERVING DIGITAL MEDIA IN CONNECTION WITH CASE INVESTIGATION OR TRIAL PREPARATION

A. AUDIO AND VIDEO DIGITAL MEDIA

1. All video records (VHS, S-VHS, DVC (mini digital video cassettes), 8mm, Hi8mm and Digital 8mm) submitted by law enforcement or the public to the District Attorney’s Office must be on VHS or S-VHS video tape or in a usable digital format (video for Windows w/Microsoft codec – 640 or 720x480 - .avi) that can be converted for editing and duplicating purposes to create prosecution work product and defense discovery.

2. All audio records originating from law enforcement agencies must be submitted to the District Attorney’s Office on standard size cassette tape in "normal" speed or in .wav format on CD. No micro-cassettes or other audio formats will be accepted, unless the materials constitute original evidence seized during the investigation.

B. PHOTOGRAPHIC DIGITAL IMAGES

1. When digital images are saved from a camera they will be stored temporarily on a computer hard disk drive or copied directly to a non-rewritable compact disc ("CD").

2. No alterations of the images whatsoever may be made while on the hard disk or in the camera.

3. The images saved to the hard disk will immediately and in their entirety be copied to a non-rewritable CD by the person who saved the images to the hard disk drive.

4. The person who saved or copied the images to the CD will immediately confirm that all files were completely and accurately copied, by comparing the file name, date and size for each digital image on the CD with those previously copied to the hard disk.
5. The person who saved or copied the images to a CD, or to the hard disk drive and copied the same images to the CD, will permanently initial and date the original CD.

6. That person will also log a permanent record of the name of the photographer, the date the images were made, and the case number.

7. The original CD will be maintained as any other evidence gathered by the investigator assigned.

8. Additional CDs may thereafter be copied and similarly marked for discovery, for the use of the trial team, and for any other necessary use.

9. The files saved to the hard disk drive will then be deleted.

10. The files on the camera memory card will then be deleted.

11. No digital image files will be permanently stored on the DA LAN if they are collected for use as evidence in a case.

12. All photographs will be made from the original CD and a chain of custody will be maintained for authentication purposes.
Index

I. Requirements for Admissibility
   A. Relevancy
   B. Authentication
   C. Secondary evidence
   D. Chain of Custody
   E. Hearsay Issues

II. Legal Issues by Technique
   A. Intercepted Communications
      1. Wire Communications
      2. Pagers
      3. Cellular/Digital Telephones
      4. Answering Machines
      5. Voice Mail Systems
      6. Pen Registers
      7. Custodial Situations
      8. Undercover Officers and Agents
   B. Surveillance Techniques
      1. Photographic
      2. Stationary Cameras
      3. Tracking Devices
      4. Thermal Imaging
      5. Sneak and Peak Search Warrants
I. Requirements for Admissibility

A. Relevancy

The evidence code provides that "relevant evidence means evidence, including evidence relevant to the credibility of a witness or hearsay declarant, having any tendency in reason to prove or disprove any disputed fact that is of consequence to the determination of the action." Evidence Code § 210.

Under this most basic principle of evidence, the trier of fact (the jury) may only hear evidence that is relevant to an issue in the case. In all criminal prosecutions, this will include:

1. The criminal act;
2. The criminal intent;
3. The identity of the defendant.

In some prosecutions, evidence of conduct of the defendant subsequent to the commission of the crime tending to show consciousness of guilt is often relevant and admissible. This type of evidence is commonly of the type of:

1. Flight from the scene of a crime;
2. Refusal to provide certain bodily fluids;
3. Intentional acts to suppress the collection of evidence;
4. Intentionally false statements.

Additionally, evidence of motive is generally relevant as evidence of the reasoning process of the defendant to explain the conduct of the defendant. People v. De La Plane (1979) 88 Cal.App.3d 223.

Photographic evidence provides circumstantial and demonstrative evidence. In a homicide, the particularly gruesome autopsy photographs may be relevant to prove malice (intent to kill) by the killer. People v. Bowen (1982) 137 Cal.App. 3d 1020. The photographs may be used to corroborate and coroner’s testimony. People v. Allen (1986) 42 Cal.3d 1222.

B. Authentication

Under the rules of evidence, "writing" means handwriting, typewriting, printing, photostating, photographing, and every other means of recording upon any tangible thing any form of communication or representation, including letters, words, pictures, sounds, or symbols, or
combinations thereof. Evidence Code § 250. Graffiti constitutes a writing under the code. Evidence Code § 1410.5

In order for any "writing" to be admissible, it must be determined to be authenticated. This means that there must be sufficient proof that the document is actually the item the party offering the document claims that it is. Evidence Code §§ 1400-1401. The manner of satisfying the authentication requirement may be accomplished in any different manner. The law recognizes the following:

4. Authentication by content when the content refers to or states matters not known by anyone but the author. Evidence Code § 1421.

C. Secondary Evidence

1. Evidence Code § 1520

(a) The content of a writing may be proved by otherwise admissible secondary evidence. The court shall exclude secondary evidence of the content of a writing if the court determines either of the following:
   (1) A genuine dispute exists concerning material terms of the writing and justice requires the exclusion.
   (2) Admission of the secondary evidence would be unfair.

2. Evidence Code § 1522

(a) In addition to the grounds for exclusion authorized by Section 1521, in a criminal action the court shall exclude secondary evidence of the content of a writing if the court determines that the original is in the proponent's possession, custody, or control, and the proponent has not made the original reasonably available for inspection at or before trial. This section does not apply to any of the following:
   (1) A duplicate as defined in Section 260.
   (2) A writing that is not closely related to the controlling issues in the action.
(3) A copy of a writing in the custody of a public entity.

(4) A copy of a writing that is recorded in the public records, if the record or a certified copy of it is made evidence of the writing by statute.

D. Chain of Custody

The concern regarding "chain of custody" issues is the likelihood that the evidence offered as evidence is the same evidence seized and has not been altered. In People v. Lucas (1995) 12 Cal.4th 415, 444, the court stated "the rules for establishing chain of custody of evidence are as follows: the burden on the party offering the evidence is to show to the satisfaction of the trial court that, taking all the circumstances into account including the ease or difficulty with which the particular evidence could have been altered, it is reasonably certain that there was no alteration. The requirement of reasonable certainty is not met when some vital link in the chain of possession is not accounted for, because then it is as likely as not that the evidence analyzed was not the evidence originally received. Left to such speculation the court must exclude the evidence. Conversely, when only the barest speculation supports an inference of tampering, it is proper to admit the evidence and let what doubt remains go to its weight."

E. Hearsay Issues

In the case of intercepted communications, the admissibility of the intercepts will depend upon its inclusion within an exception of the hearsay rule. As a general rule, statements of the defendant will be admissible as a party admission. Evidence Code § 1220. In those situations where the actual speaker is not a defendant at the trial, the statement may be admissible as a co-conspirator's statement. Evidence Code § 1223. In either situation, the credible identification (authentication) of the party is critical.
II. Legal Issues by Technique

A. Intercepted Communications

1. Wire Communications

   A. Penal Code § 629.50
   Under California Law, the interception of a wire, electronic
digital pager, or electronic cellular telephone communication shall
only be made by Court Order pursuant to this statute.

   "Electronic digital pager communication" means any tone or
digital display or tone and voice pager communication. Penal Code
§ 629.51 (a).

   "Electronic cellular telephone communication" means any
     cellular or cordless radio telephone communication. Penal Code §
629.51 (b).

B. Qualifying Crimes

The Order to intercept wire communication can only be
issued for the investigation of the following crimes:

1. Importation, possession for sale,transportation, manufacture, or sale of
controlled substances in violation of Section
11351, 11351.5, 11352, 11378, 11378.5,
11379, 11379.5 or 11379.6 with respect to
heroin, cocaine, PCP, methamphetamine, or
analogs when amount exceeds 10 gallons by
liquid volume or 3 pounds by weight;

2. Murder, solicitation to commit murder, the
commission of a crime involving the bombing
of private or public property or aggravated
kidnapping;

3. Conspiracy to commit any of the above crimes.

C. Civil Penalties for Illegal Intercept
Penal Code § 629.86

Any person’s wire, electronic digital pager or
electronic cellular telephone communication may sue
anyone who intercepts, discloses, uses or procures any
other person to intercept, disclose or use the communication.

The plaintiff can receive actual damages at a rate of $100 a day for each day of the violation or $1,000 whichever is greater.

Punitive damages and reasonable attorney’s fees and other litigation costs.

D. Prohibition of Covert Entry
Penal Code § 629.89

No order shall permit either directly or indirectly authorize covert entry into or upon the premises of a residential dwelling, hotel room, or motel room for installation or removal of any device or for other purpose.

E. POST Certification
Penal Code § 629.94

Investigative and Law Enforcement Officers must complete a certification course to apply for intercept orders, conduct intercepts, and to use the communications or evidence derived from the intercept.

F. Exclusionary Rule

1. General Rule

Exclusionary Rule prohibits the use of any statements or evidence derived from an unauthorized wire intercept.

2. Third Party Interception

The unauthorized interception of wire communications by third parties, without law enforcement knowledge, is subject to exclusion in any subsequent legal proceeding. People v. Otto (1992) 2 Cal.4th 1088.

3. Impeachment Exception

It is unclear whether courts will permit the use of unauthorized wire intercepts for impeachment purposes; however, the court did permit the use of unauthorized wire

However, it should be assumed until clarified by the courts that illegal intercepts are inadmissible in all proceedings for all purposes.

2. Pagers

A. General Rule

The interception of electronic pager requires the authorization of and compliance with Penal Code § 629.50 et seq.

B. Broadcast or Tone-Only Pagers


3. Cellular/Digital Telephones

A. General Rule

The interception of cellular and digital telephones requires the authorization of and compliance with Penal Code § 629.50 et seq.

4. Answering Machines

A. Expectation of Privacy

As a general rule, people have an expectation of privacy in their telephone calls and answering machines. *People v. Harwood* (1977) 74 Cal.App.3d 460.

B. Probable Cause Standard

Upon a showing of probable cause, search warrants may include the authority to answer telephone calls and
seiZe the tapes from telephone answering machines. 

5. Voice Mail Systems

A. Interception under Title III

Unconsented retrieval of recorded voice mail messages constituted an interception under the federal Wiretap statutes. United States v. Smith, 155 F.3d 1051 (9th Cir. 1998)

B. Third Party Retrieval

Federal Wiretap statutes precludes the use of unauthorized intercepted communications and any evidence derived therefrom. Thus, even the innocent third party retrieval of voice mail messages are excluded under the statute. United States v. Smith, 155 F.3d 1051 (9th Cir 1998)

6. Pen Registers

A. Device

The Pen Register records the number(s) dialed from a specific telephone and records the number for identification. The device is connected to the telephone line and records numbers dialed and when the telephone is picked up and replaced.

B. Expectation of Privacy

An individual does not have an expectation of privacy in the numbers dialed from their telephone that go out into the world. Smith v. Maryland (1979) 442 U.S. 735. People v. Larkin (1987) 194 Cal.App.3d 650

C. Rational

When an individual dials a telephone the number they dial is transferred throughout the communication system until it locates the subscriber desired. The person dialing has no control over this activity thus they cannot have an
expectation of privacy over the information transmitted: the number dialed.

D. Search Warrant or Court Order

As a practical matter, most agencies obtain search warrants, or court orders, for the placement of a pen register. Although there is no expectation of privacy in the number dialed, the utility companies will not participate without some court authorization. Should you decide to use a Search Warrant, the utility company may only participate for the time period prescribed in Penal Code § 1534. In People v. Larkin (1987) 194 Cal.App.3d 650, the court did not suppress evidence collected on a warrant 30 days old.

7 Custodial Situations

A. Expectation of Privacy

Courts will recognize an expectation of privacy in those areas which society is prepared to recognize as reasonable. As a general rule, "the recognition of privacy rights for prisoners in their individual cells simply cannot be reconciled with the concept of incarceration and the needs and objectives of penal institutions. Hudson v. Palmer (1984) 468 U.S. 517, 526.

B. Individual Cells


C. Back Seat of Police Vehicle

Arrestees do not have an expectation of privacy in the back seat of a police vehicle that they could conduct a conversation with a suspected accomplice free from police eavesdropping. People v. Crowson (1983) 33 Cal.3d 623.
D. Jail Visiting Areas

1. General Rule


2. Privileged Communication

Penal Code § 636(a) states it is a felony to eavesdrop upon the privileged communication between an incarcerated individual and their attorney, religious advisor or licensed physician.

3. Not Privileged Situations


4. Creating the Expectation of Privacy

In *North v. Superior Court* (1972) 8 Cal.3d 301, the court held that the private conversation between an incarcerated husband and his wife was illegally seized as a violation of a reasonable expectation of privacy.

The court noted that:

1. Detective offered his private office for the location of the conversation.
2. The detective left the office and left the two alone.
3. The detective closed the door after he left.

The *North* Court reasoned that the officers lulled the defendant and his wife into believing that their conversation would be confidential. *8 Cal.3d at 311-2.*

E. Mail Intercepts

1. General Rule

Most policy and procedure established for the purpose of preserving jail security, to include the monitoring of mail must yield to the Fourth Amendment reasonable expectation of privacy. *People v. McCaslin* (1986) 178 Cal.App.3d 1, 7.

2. Specific Situations

A. Internal Mail between Inmates

Reasonable to intercept and read the mail between inmates. *People v. McCaslin* (1986) 178 Cal.App.3d 1, 7.

B. Internal Mail between Spouses


C. Inspection of Mail for Escape Plans


9. Undercover Officers and Agents

It is legal and permitted to place a "wire" on an undercover civilian agent who enters a private location. *United States v. White* (1971) 401 U.S. 745.
It may be a violation of a codefendant's Fifth and Sixth Amendment rights to wire an informant for the purpose to collecting evidence. *Miassiah v United States* (1964) 377 U.S. 201.

B. Surveillance Techniques

1. Photographic Evidence

   A. Relevancy

   Photographic evidence will be admissible in court when it will assist the jury in determining a factual issue in the trial. Any type of demonstrative evidence is admissible so long as the it is properly authenticated prior to admission. *People v Rodriguez* (1994) 8 Cal.4th 1060.

   B. Authentication

   1. Physical Dimension of Crime Scene

   Daytime videotaping of the physical dimensions of a crime scene held admissible even though the crime occurred at night. *People v Rodriguez* (1994) 8 Cal.4th 1060

   2. Lighting Conditions During Crime

   Photographs of crime scene at 7:30 pm many months after the crime for the purpose showing the lighting conditions at 2:00 am is inadmissible. Court reasoned it was incumbent upon the prosecution to lay a proper foundation at least by having the pictures taken at the same hour of the morning as the incident. *People v Vaiza* (1966) 244 Cal.App.2d 121, 127.

   3. Reaction Times of Parties

   In lawsuit over train crossing collision with vehicle, party offered color film of train approaching crossing. Film made in daylight of a nighttime collision and using different type of engine.

4. Photos 3 Years After Event

The fact that the photos were taken 3 years after the event is not dispositive when they are otherwise authenticated. Court held "passage of time alone ... will not warrant its exclusion from evidence, if the other factors of necessary authentication are present." *La Gue v. Delgaard* (1956) 138 Cal.App.2d 346, 348.

2. Stationary Camera

A. Expectation of Privacy

1. Plain View Doctrine

Officers are permitted to conduct a visual search of their surroundings from a location where they have a legal right to be present. *Guidi v. Superior Court* (1973) 10 Cal.3d 1

Forest Service officers discover an outdoor marijuana site; defendants are photographed tending to plants. Court holds "we reject the notion that the visual observations of the site became unconstitutional merely because law enforcement chose to use a more cost-effective 'mechanical eye' to continue the surveillance." Further, "the use of photographic equipment to gather evidence that could be lawfully observed by a law enforcement officer does not violate the Fourth Amendment. The use of a motion activated camera under these circumstances appears to us to be a prudent and efficient use of modern technology." *United States v. McIver* (9th Cir. 1999) ***F.3d*** (Decided 8-6-99)

2. No Independent Grounds of Privacy

News photographer who videotaped judge for news story while walking to his car from his house did not invade the protected
privacy of the judge when the photographs were taken in the public view. 


3. Enhanced Physical Abilities

A. General Rule

The use of binoculars or aural aids is not itself an invasion of expectation of privacy so long as the officer is in a location where they may legally be. Cooper v. Superior Court (1981) 118 Cal.App.3d 499.

The use of binoculars is permissible so long as the item viewed is something that could have been seen with the naked eye. Dow Chemical v. United States (1986) 476 U.S. 731, 748.

B. Use of Artificial Lighting

Use of flashlight into a car is permissible and not an invasion of privacy. People v. Rogers (1978) 21 Cal.3d 542.

C. Ultraviolet Light

Use of ultraviolet light to inspect hands for powder is a search under the Fourth Amendment. United States v. Kenaan (1st Cir.) 496 F.2d 181.

2. Use of Sophisticated Equipment

EPA use of aerial surveillance equipment from the navigable airspace over a 2000 acre industrial plant is not a search prohibited by the Fourth Amendment. Dow Chemical Company v. United States (1986) 476 U.S. 227.
3. Official Government Privilege (Evidence Code § 1040)

A. Governmental Privilege

(a) As used in this section, "official information" means information acquired in confidence by a public employee in the course of his or her duty and not open, or officially disclosed, to the public prior to the time the claim of privilege is made.

(b) A public entity has a privilege to refuse to disclose official information, and to prevent another from disclosing official information, if the privilege is claimed by a person authorized by the public entity to do so and:

(1) Disclosure is forbidden by an act of the Congress of the United States or a statute of this state; or

(2) Disclosure of the information is against the public interest because there is a necessity for preserving the confidentiality of the information that outweighs the necessity for disclosure in the interest of justice; but no privilege may be claimed under this paragraph if any person authorized to do so has consented that the information be disclosed in the proceeding. In determining whether disclosure of the information is against the public interest, the interest of the public entity as a party in the outcome of the proceeding may not be considered.

B. Applies to Surveillance Locations

Covert surveillance location used by police to investigate narcotics sales was information that could be protected from disclosure by statutory privilege for information acquired in confidence by public employee in course of their duties.

Officer only had to disclose that he was 50 yards away on an overcast day with an unobstructed view. *Hines v Superior Court* (1988) 203 Cal.App.3d 1231

Exact location not disclosed when testimony of officer was that from less the 100 yards away he used 35 power binoculars and observed the defendant who was dressed uniquely. *In re Sergio M.* (1993) 13 Cal.App.4th 809

3. Tracking Devices

A. Expectation of Privacy

Retrieval of tracking signal from the inside of a location where a party has an expectation of privacy without a search warrant is unreasonable.
The placement of a tracking device in legally purchased ether being sold to defendant was unreasonable especially when the signals were monitored while the device was inside the defendant's residence. *United States v. Karo* (1984) 468 U.S. 705.

B. Public Roadways


C. Government Property

Placement of a tracking device in federal mail pouches of carrier suspected of mail theft okay insofar as the defendant had no recognizable privacy interest in the governmental property. *United States v. Jones* (4th Cir 1994) 31 F.3d 1304.

D. Stolen Property

Payless private agents placed tracking devices in bank deposits bags. The bags were tracked to a motel room where officers made a warrantless entry to recover the stolen property. Court held the defendants did not have a recognizable expectation of privacy in the stolen private merchandise. *People v. Erwin* (1997) 55 Cal.App.4th 15.

4. Thermal Imaging

A. Technology

The infrared thermal scan is a non-intrusive device which emits no rays or beams and shows a crude visual image of the heat being radiated from the outside of a location. The device cannot show any people or activity within the walls of a structure and records only the heat emitted from a structure. *United States v. Kyllo* (9th Cir 1999) __ F.3d __

B. Expectation of Privacy

So long as the technology does not reveal the intimate details of the activities inside the structure, there is no invasion of the reasonable expectation of privacy via use of the thermal imager. *United States v. Kyllo*.

Other Federal Courts in Accord:

*United States v. Cusumano* (10th Cir 1996) 83 F.3d 1247
5. Sneak and Peak Search Warrants

During an investigation, investigators may seek to enter and search a location surreptitiously for the purpose of noting, photographing and/or recording objects without the knowledge of the targets.

The court may, based upon a factually basis good cause:

1. Authorize covert or surreptitious entry
2. Delay the giving of notice to the occupants of the location
3. Permit the recordation of specific objects identified in the warrant affidavit without seizure.

Delia v. United States, 441 U.S. 238 (1978),
United States v. Freitas, 800 F.2d 1451 (9th Cir. 1988)

Affidavit must include:

1. Statement of probable cause for search and recording of objects;
2. Needs for surreptitious entry
   Other investigatory avenues failed
   Other investigatory avenues unavailable
3. Need for nighttime service
4. Justification for need to delay notice and extension

Warrant must include:

1. Description of premises
2. Authorization of surreptitious entry
3. Authorize exemption of notice and receipt
4. Specific acts authorized
   Search but no seizure
   Search for objects to include listening to messages
   Photograph, videotaping, etc of items
August 7, 2002

TO ALL CALIFORNIA DISTRICT ATTORNEYS

RE: Amended Advisory letter on People v Loyd

On June 3, 2002, I sent out an advisory letter on the recent California Supreme Court decision in People v Loyd (2002) 27 Cal.4th 997. In that advisory, I noted that there remained an issue as to the monitoring of a jail detainee’s outgoing telephone calls and that "California is a state which severely limits the offenses for which a prosecutor may obtain a judicially authorized wiretap order (see Penal Code § 629.52) and requires two-party consent before calls (on other than intra-jail telephone systems) may be monitored."

Shortly after this letter was sent out, Alameda County District Attorney Tom Orloff contacted me to express his concern about the position I had taken regarding the requirement for two-party consent. I agreed to reexamine this question, and I have now concluded that my opinion on the need for two-party consent was too conservative. I agree with District Attorney Orloff that, although there are no cases directly on point, a strong argument can be advanced that, under the law enforcement exception of Penal Code § 633, two-party consent is not required for a designated law-enforcement officer to monitor and record a jail detainee’s outbound telephones calls. This position is viable because there is sufficient case law to support an argument that, prior to 1967 when the two-party consent restriction in Penal Code § 632 was enacted, law enforcement could have monitored and recorded such calls without the need for two-party consent, either on a theory that there was no reasonable expectation of privacy in such calls, or under a theory that the implied consent of one party was sufficient.

I apologize for any confusion that my original advisory letter may have caused.

Sincerely,

ROBERT R. ANDERSON
Chief Assistant Attorney General

For BILL LOCKYER
Attorney General

- 3815 -
THE PEOPLE, Plaintiff and Respondent, 
 v. 
CHRISTINE LOYD, Defendant and Appellant.

No. S092653.

Supreme Court of California

May 6, 2002.

SUMMARY

Defendant was convicted by jury of two counts of first degree murder and one count of arson. While defendant was in jail awaiting trial, the prosecutor requested the recording of defendant’s conversations with her nonattorney visitors. The trial court denied defendant’s motions to suppress the recorded conversations. (Superior Court of Alameda County, No. 127214, Philip V. Sarkisian, Judge.) The Court of Appeal, First Dist., Div. Four, No. A080542, affirmed, finding no federal constitutional violation, and thus no basis for remedy.

The Supreme Court affirmed the judgment of the Court of Appeal. The Court held that the prosecutor’s request to secretly monitor and record defendant’s unprivileged jail conversations with her visitors solely for the purpose of gathering evidence, and the prosecutor’s subsequent use of the tape, did not constitute misconduct under state law. Although a 1982 opinion by the California Supreme Court held that monitoring inmate conversations was barred unless necessary for security purposes, that opinion had been superseded by statute at the time of the surveillance of defendant. Under Pen. Code, § 2600, as amended in 1994, a person sentenced to imprisonment may be deprived of such rights, and only such rights, as is reasonably related to legitimate penological interests. The amendment reflected the Legislature’s desire to repeal the expansive protections afforded California inmates and replace them with the more limited protections available under federal law. Thus standard permits restrictions on inmates’ activities whenever they are reasonably related to proper goals. The Legislature intended to restore the former law regarding inmates’ rights. Any restrictions on inmates’ rights that were lawful prior to the Supreme Court’s 1982 opinion, such as the recording of an inmate’s conversation as took place in this case, are lawful under the current test.

[See 4 Witkin & Epstein, Cal. Criminal Law (3d ed. 2004) Illegally Obtained Evidence, § 352; West’s Key Number Digest, Prisons § 216(a).]

HEADNOTES

(1a, 1b) Penal and Correctional Institutions § 16--Prisons and Prisoners--Right to Privacy--Recording Conversations of Inmate; Criminal Law § 359--Evidence--Intercepted Communications

The prosecutor’s request to secretly monitor and record a murder suspect’s unprivileged jail conversations with her visitors solely for the purpose of gathering evidence, and the prosecutor’s subsequent use of the tape, did not constitute misconduct under state law. Although a 1982 opinion by the California Supreme Court held that monitoring inmate conversations was barred unless necessary for security purposes, that opinion had been superseded by statute at the time of the surveillance of defendant. Under Pen. Code, § 2600, as amended in 1994, a person sentenced to imprisonment may be deprived of such rights, and only such rights, as is reasonably related to legitimate penological interests. The amendment reflected the Legislature’s desire to repeal the expansive protections afforded California inmates and replace them with the more limited protections available under federal law. Thus standard permits restrictions on inmates’ activities whenever they are reasonably related to proper goals. The Legislature intended to restore the former law regarding inmates’ rights. Any restrictions on inmates’ rights that were lawful prior to the Supreme Court’s 1982 opinion, such as the recording of an inmate’s conversation as took place in this case, are lawful under the current test.

[See 4 Witkin & Epstein, Cal. Criminal Law (3d ed. 2004) Illegally Obtained Evidence, § 352; West’s Key Number Digest, Prisons § 216(a).]

(2) Penal and Correctional Institutions § 16--Prisons and Prisoners--Right to Privacy--Monitoring Conversations--Conversations in Jail and Police Cars

Police officers may monitor conversations in jail as they may monitor conversations in police cars. There is no distinction between the two locations.
regarding an individual's reasonable expectations of privacy in his or her communications.

COUNSEL

Jo Anne Keller for Defendant and Appellant.

Kenneth I. Chapman, Public Defender (Ventura) and Michael C. McMahon, Chief Deputy Public Defender, for California Public Defender Association *999 and the Public Defender of Ventura County as Amicus Curiae on behalf of Defendant and Appellant.

Alan L. Schlosser for American Civil Liberties Union of Northern California as Amicus Curiae on behalf of Defendant and Appellant.

John T Phillipsborn for California Attorneys for Criminal Justice as Amicus Curiae on behalf of Defendant and Appellant.

Bill Lockyer, Attorney General, David P Druhlner, Chief Assistant Attorney General, Ronald A. Bass, Assistant Attorney General, Rene A. Chacon, Bridget Billeter and William Kruitwels, Deputy Attorneys General, for Plaintiff and Respondent.

George Palmer, Thomas J. Orloff, District Attorney (Alameda) and A. Mark Hutchins, Deputy District Attorney, for California District Attorneys Association as Amicus Curiae on behalf of Plaintiff and Respondent.

BROWN, J.

In this case we consider whether secretly monitoring and recording an inmate's unprivileged jail conversations with her visitors, solely for the purpose of gathering evidence, constituted prosecutorial misconduct by violating De LANCE v. Superior Court (1982) 31 Cal.3d 865 [183 Cal.Rptr. 866, 647 P.2d 142] (De LANCE). Because we decide De LANCE had been superseded by statute at the time of the taping, we find the prosecutor's request for and use of the tape did not constitute misconduct under state law.

I. Factual and Procedural Background

Christine Loyd was convicted by jury of two counts of first degree murder (Pen. Code, § 187) [FN1] and one count of arson (§ 451, subd. (c)), and was sentenced to prison for a term of 55 years to life.

FN1 Unless otherwise indicated, all further statutory references are to the Penal Code.

Before her trial began, defendant sought a ruling on the legality of the taping of defendant's personal visits and telephone calls. [FN2] After the prosecution noted defendant's motion failed to request a remedy, defendant formally moved for dismissal of the charges or recusal of the prosecutor. Defendant *1000 alleged the prosecutor violated the rule of De LANCE, supra, 31 Cal.3d 865, which bars monitoring of inmate conversations unless necessary for security purposes.

FN2 Our decision today concerns the effect of only California law. As Justice Moreno's concurring opinion observes, there may be a federal basis, the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. § 2510 et seq.), for suppressing the tapes of the telephone conversations. The federal law, however, has not been the basis of defendant's motions or appeals, the Court of Appeal decision or our grant of review. We therefore express no opinion on its applicability.

The parties stipulated to certain facts. Defendant was in jail awaiting trial for the murder of Virginia Baily. The prosecutor requested the recording of defendant's conversations with her nonattorney visitors. In response to this request, the sheriff's department provided the prosecutor with tapes of conversations between defendant and three visitors, Kristen Albertson, Dave DeWolf and Ann Argabrite. The prosecutor also requested and received tapes of telephone conversations defendant had with her brother, Philip Loyd, and with Ann Argabrite. The recorded communications occurred between March 26, 1996, and June 30, 1996. There was no taping of any conversation between defendant and her attorney or anyone retained by her attorney The prosecutor requested this taping to gather evidence for the prosecution of Virginia Baily's murder, and to gain an indictment and subsequently prosecute defendant for the murder of her mother, Myrtle Loyd.

The trial court denied defendant's suppression motions. The jury convicted defendant on both counts of murder and one count of arson. Defendant appealed.

The Court of Appeal discussed our De Lrance decision at length. The court noted De Lrance arose out of a civil suit seeking declaratory and injunctive relief from what had been the routine practice of recording conversations between inmates and visitors. Prior to De Lrance, we had recognized a right of confidentiality only for protected communications, like those between an inmate and counsel. (North v. Superior Court (1972) 8 Cal.3d 301, 308-311 [104 Cal.Rptr. 833, 502 P.2d 1305, 57 A.L.R.3d 155] (North); see also § 636 [forbidding eavesdropping on communications between inmate and attorney, religious adviser or physician]). In De Lrance, supra, 31 Cal.3d at page 885, however, we concluded former sections 2600 and 2601 extended the protection of confidentiality to unprivileged communications, unless monitoring was necessary for the security of the institution or the public.

The Court of Appeal noted the difficulty involved in applying De Lrance. "The decision in De Lrance may well have raised more questions than it answered, including the nature and origin of the right protected, the extent to which it depends on the subjective expectations of prisoners and visitors, the extent to which it is subject to modification or abolition by legislative action, *1001 and-of foremost importance here-the nature of the remedy, if any; to be granted by a trial court presiding over a criminal prosecution in which the prosecutor has recorded the defendant's conversations in violation of De Lrance."

The Court of Appeal opinion also noted the concerns of the De Lrance dissenters. "The practice of monitoring an inmate's conversations is (1) reasonably necessary to maintain jail security, and (2) that a person incarcerated in a jail or prison possesses no justifiable expectation of privacy." (De Lrance, supra, 31 Cal.3d 865, 879 (dis. opn. of Richardson, J.); see id. at p. 882 (dis. opn. of Mosk, J.).) Justice Richardson also quoted our opinion in North, supra, 8 Cal.3d at page 309: "A man detained in jail cannot reasonably expect to enjoy the privacy afforded to a person in free society. His lack of privacy is a necessary adjunct to his imprisonment .... " (De Lrance, at p. 881 (dis. opn. of Richardson, J.).)

The Court of Appeal held the tape recording did not violate the Fourth, Fifth or Sixth Amendment to the United States Constitution, and thus suppression was not an available remedy. The court thus stated that defendant's "only coherent theory of error is that the prosecutor's misconduct was such an egregious violation of her rights as to 'shock the conscience' and effect a denial of due process under the federal Constitution." The opinion cited Proposition 8 (Cal. Const., art. I, § 28, subd. (d)), "which prohibits the suppression of evidence except where it is compelled by federal authority." [FN3] Finding no federal constitutional violation, and thus no basis for remedy, whether suppression, dismissal or recusal, the Court of Appeal noted that the unresolved De Lrance issues "may deserve the attention of the Supreme Court, especially in light of recent statutory amendments [to section 2601]."

FN3 The court refused to find that the federal Omnibus Crime Control and Safe Streets Act of 1968 compelled suppression.

Justice Poche dissented, disagreeing with the majority's conclusion that there was no available remedy. The dissent construed the tape as a denial of defendant's right to due process of law, warranting reversal and retrial. Justice Poche also found that the telephone tapping violated federal wiretap law. We granted review on the limited question of whether the trial court erred in not dismissing the information or recusing the prosecutor for the asserted De Lrance violation.

II. Discussion

(1a) Defendant contends the surreptitious tape recording of conversations between her and her visitors violated De Lrance and warranted a *1002 remedy-either dismissal, recusal or suppression. Our analysis of the issue persuades us that the amendments noted by the Court of Appeal have abrogated the statutory basis for De Lrance. Indeed, the Legislature has acted to restore the pre-De Lrance state of the law. Accordingly, we find the taping of the conversations between defendant and her visitors did not violate California law.

A. The Legacy of Lrance: Jail Inmates Do Not Enjoy a Justifiable Expectation of Privacy
The United States Supreme Court addressed this issue 40 years ago in Lanza v. New York (1962) 370 U.S. 139 [82 S.Ct. 1218, 8 L.Ed.2d 384] (Lanza). Jail officials secretly tape-recorded a conversation between Lanza and his brother, an inmate, without their knowledge. (Id. at p. 141 [82 S.Ct. at pp. 1219-1220].) The court rejected Lanza's contention that the tape was the product of a Fourth Amendment violation. It distinguished the jail from those other settings that could implicate the right to be free from unreasonable search and seizure. "To say that a public jail is the equivalent of a man's 'house' or that it is a place where he can claim constitutional immunity from search or seizure of his person, his papers, or his effects, is at best a novel argument .... [W]ithout attempting either to define or to predict the ultimate scope of Fourth Amendment protection, it is obvious that a jail shares none of the attributes of privacy of a home, an automobile, an office, or a hotel room. In prison, official surveillance has traditionally been the order of the day." (Lanza, at p. 143 [82 S.Ct. at pp. 1220, 1221], fn. omitted.)

The Lanza doctrine shaped Congress's creation of the Omnibus Crime Control and Safe Streets Act of 1968. Title 18 United States Code section 2510(2), part of the wiretap law, defines a protected oral communication as one "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." The legislative history indicates that although Congress did not intend that the place of the communication determine the justifiability of the expectation, "[n]evertheless, such an expectation would clearly be unjustified in certain areas; for example, a jail cell (Lanza v. New York, 82 S.Ct. 1218, 370 U.S. 139 (1962)) ...." (Sen.Rep. No. 1097, 90th Cong., 2d Sess. (1968), reprinted at 1968 U.S. Code Cong. & Admin. News, p. 2178.)

We embraced the principle that a suspect's custodial conversations did not enjoy a justifiable expectation of privacy. Although we protected a defendant's right to privacy regarding his communications with counsel (In re Jordan (1972) 7 Cal.3d 930, 937-938, fn. 3 [103 Cal.Rptr. 849, 500 P.2d *1003 873]; People v. Lopez (1963) 60 Cal.2d 223, 248 [32 Cal.Rptr. 424, 384 P.2d 16]) or where jail officers acted so that the suspect "and his wife were lulled into believing that their conversation would be confidential" (North, supra, 8 Cal.3d at p. 311), we affirmed the general rule that "[a]bsent such unusual circumstances, [inmates and their visitors] can have no reasonable expectation that their jailhouse conversations will be private." (People v. Hill (1974) 12 Cal.3d 731, 765 [117 Cal.Rptr. 393, 528 P.2d 1], overruled on other grounds in People v. DeVauhn (1977) 18 Cal.3d 889, 896, fn. 5 [135 Cal.Rptr. 786, 558 P.2d 872].)


B. The Lawfulness of Inmate Monitoring and Recording Prior to De Landa

Prior to our 1982 De Landa opinion, inmate monitoring and recording as occurred below was lawful in California and the rest of the country. In addition to rejecting the claims that monitoring violated an inmate's justifiable expectation of privacy, California courts also rejected former section 2600 as a basis for insulating custodial conversations from oversight. We described the import of that statute: "In this state we have long since abandoned the medieval concept of strict 'civil death' and have replaced it with statutory provisions seeking to ensure that the civil rights of those convicted of crime be limited only in accordance with legitimate penal objectives. The 1968 amendments ... which resulted in the enactment of section 2600 in its present form, represent the most recent legislative effort in this direction." (In re Harrell (1970) 2 Cal.3d 675, 702 [87 Cal.Rptr. 504, 470 P.2d 640] (Harrell), italics added.)

The Harrell standard allowed the secret recording of custodial conversations. In Estrada, supra, 93 Cal.App.3d 76, the defendant's sister, and, on another occasion, his brother-in-law, visited him in
Most apposite to the instant case is Owens, supra, 112 Cal.App.3d 441. Police arrested Owens and another suspect, who offered conflicting statements. They were placed together in an interview room where they made inculpatory statements that were secretly recorded. (Id. at p. 444.) The Court of Appeal affirmed the validity not only of the taping but also of what we later characterized as the public interest in detecting a suspect's fabrication. (Donaldson v. Superior Court (1983) 35 Cal.3d 24, 33, fn. 6; [196 Cal.Rptr. 704, 672 P.2d 110] (Donaldson) (plur. opn. of Broussard, J.).) "The monitoring system ... was used to overhear a discussion between two recently arrested felony suspects who had just made factually divergent statements in separate interviews. Thus, in addition to the compelling interest in maintaining jail security we must consider the public interest in acting on a well-founded suspicion that the detainees would take the opportunity to get their stories straight and that their conversation would touch on criminal activity." (Owens, at p. 449.)

Therefore, prior to De Lancie, the prevailing law recognized as legitimate the "interest in ferreting out and solving crimes." (People v. Seaton (1983) 146 Cal.App.3d 67, 81, fn. 11 [194 Cal.Rptr. 33], citing Owens, supra, 112 Cal.App.3d at pp. 449-450.) We thus observed that "[p]rior to De Lancie, the fact that a particular conversation was monitored not for security purposes but to gather evidence did not argue against admissibility." (Donaldson, supra, 35 Cal.3d at p. 33, fn. omitted.) This principle conformed to federal law, which also found this motive legally insignificant. The Ninth Circuit Court of Appeals approved taping in a case where police placed two codefendants in a room "in the hope that the two would discuss the crime and make some incriminating admissions." (Williams v. Nelson (9th Cir. 1972) 457 F.2d 376, 377 (Nelson.) [FN4] Had the taping in this case occurred prior to De Lancie, there would have been no valid basis for objection.

FN4 Nelson adopted an even more deferential position toward jailhouse taping than Owens, masmuch as the room in which the Nelson defendants were placed was "apparently private" (Nelson, supra, 457 F.2d at p. 377) which, under California law, could have been grounds for invalidating the taping. (See North, supra, 8 Cal.3d at p. 311.)

C. Procunier and the Demise of Harrell

The Harrell standard had a limited lifespan, thanks to prodding from the United States Supreme Court. Although the Court of Appeal, citing Harrell, had allowed the censoring of inmate mail to parties other than counsel (Yarish v. Nelson. (1972) 27 Cal.App.3d 893, 898 [104 Cal.Rptr. 205]), the high court restricted this practice in Procunier v. Martinez (1974) 416 U.S. 396 [94 S.Ct. 1800; 40 L.Ed.2d 224] (Procunier), [FN5] which found former section 2600 inadequate to protect the constitutional rights at stake. (Procunier, at pp. 403-404 [94 S.Ct. at pp. 1806-1807].) The Procunier court, considering the First Amendment rights involved, barred censorship of mail for the purpose of suppressing criticism of prison authorities. Instead, the court required that prison officials "must show that a regulation authorizing mail censorship furthers one or more of the substantial governmental interests of security, order, and rehabilitation. Second, the limitation of First Amendment freedoms must be no greater than is necessary or essential to the protection of the particular governmental interest involved." (Procunier, at p. 413 [94 S.Ct. at p. 1811].) Thus, prison regulations involving mail had to be "generally necessary" to protect security, order or rehabilitation. (Id. at p. 414 [94 S.Ct. at pp. 1811-1812].) [FN6] Notably, the decision rested not on the free speech rights of the inmate (the court declined to decide the extent to which these rights survived incarceration) but on the rights of those relatives and friends outside the prison who wished to correspond with the inmate. (Procunier, at pp.
two respects: (1) the statute omitted rehabilitation from the list of permitted goals; [FN7] and (2) the statute provided for the same strict scrutiny regardless of whether the right was protected by the United States Constitution. Additionally, the Legislature added section 2601, which, in former subdivision (d), granted prisoners the right to have personal visits, subject to reasonable security restrictions. [FN8] (Stats. 1975, ch. 1175, § 3, pp. 2897-2898.) These statutory amendments formed the basis for De Lanoe's invalidation of the formerly lawful practice of monitoring and recording custodial conversations.

FN7 Additionally, whereas Procunier recognized the propriety of curtailing speech to protect "order" [Procunier, supra, 416 U.S. at p. 413 [94 S.Ct. at p. 1811]], overruled on other grounds by Thornburgh v. Abbott, supra, 490 U.S. 401, the statute focused on "the reasonable protection of the public" (former § 2600, as amended by Stats. 1975, ch. 1175, § 3, p. 2897). These two interests may be similar.

FN8 The former statute did not insulate these visits from 'monitoring, in contrast to section 2600, subdivision (b), which, since 1975, has protected the right "[t]o correspond, confidentially, with any member of the State Bar or holder of public office."

D. De Lanoe

De Lanoe was the result of a suit for declaratory and injunctive relief from the practice of monitoring and recording inmates' [FN9] conversations for the purpose of gathering evidence for use in prosecutions. (De Lanoe, supra, 31 Cal.3d at p. 867.) [FN10] The De Lanoe court recalled the Harrell standard, under which inmate rights could "be limited only in accordance with *1007 legitimate penal objectives," (De Lanoe, at p. 871, quoting Harrell, supra, 2 Cal.3d at p. 702) but found that standard was superseded by the 1975 amendment to section 2600. We quoted the amended provision, italicizing the words "necessary in order to provide for the reasonable security of the institution" to emphasize the shift in the law away from the former standard. (De Lanoe, at p. 870.) [FN11] The De Lanoe majority observed the recordings violated this standard if, as the complaint alleged, they "are intended not to enhance or preserve prison security, but rather to obtain evidence for use by investigatory
and prosecuting agencies in search of convictions." (Id. at p. 873.)

FN9 The De Lance case concerned pretrial county jail detainees rather than convicted prisoners in state institutions. We reasoned, however, that pretrial detainees deserved "rights at least equivalent" to those enjoyed by convicted felons. (De Lance, supra, 31 Cal.3d at p. 872.)

FN10 Because the respondent sheriff filed a demurrer, we had no opportunity to determine the factual question of whether and to what extent the monitoring and taping was for security or investigative purposes. (De Lance, supra, 31 Cal.3d at p. 868.)

FN11 The court thus rejected dictum in North, supra, 8 Cal.3d at page 312; approving comparable recording, because North predates the 1975 section 2600 amendment. (De Lance, supra, 31 Cal.3d at p. 874.)

Although the plaintiffs had alleged violations of the federal and California Constitutions, as well as the federal wiretap law (18 U.S.C. §§ 2510-2520), we based our ruling solely on a ground omitted from the complaint: sections 2600 and 2601. "[T]he provisions of Penal Code sections 2600 and 2601 are dispositive of the issues presented here." (De Lance, supra, 31 Cal.3d at p. 870.) Nothing in the decision otherwise altered the traditional understanding that inmates do not enjoy a justifiable expectation of privacy in their custodial conversations. On the contrary, as Justice Mosk's dissent observed, "The concept of one purporting to enjoy privacy while he is under legally authorized supervision would appear to be a monumental anomaly." (De Lance, supra, 31 Cal.3d 865, 882 (dis. opn. of Mosk, J.).) [FN12]

FN12 De Lance expressly declined to consider a constitutional basis for its holding (De Lance, supra, 31 Cal.3d at p. 877, fn. 13). We have usually, but not uniformly, recalled the holding's limited basis. (Compare People v. Champion (1995) 9 Cal.4th 879, 912 [39 Cal.Rptr.2d 547, 891 P.2d 93] [De Lance "held that sections 2600 and 2601 prohibit police from monitoring"]; People v. Gallego (1990) 52 Cal.3d 115, 169 [276 Cal.Rptr. 679, 802 P.2d 169] ["[I]mposing on statutory grounds, we held ... the police may not monitor"]; People v. Carrera (1989) 49 Cal.3d 291, 326 [261 Cal.Rptr. 348, 777 P.2d 121] [describing De Lance as "holding that the monitoring ... was barred by sections 2600 and 2601"]; People v. Phillips (1985) 41 Cal.3d 29, 79 [222 Cal.Rptr. 127, 711 P.2d 423] [De Lance expressly declined to base our decision on federal or state constitutional grounds, finding it sufficient to rest it on section 2560 ... and section 2601]; People v. Crittendon (1983) 33 Cal.3d 623, 630 [190 Cal.Rptr. 165, 660 P.2d 389] (phr. opn. of Kaus., J.) ["In De Lance we held that sections 2600 and 2601 accord ... a statutory right to privacy"]; with People v. Edelbacher (1989) 47 Cal.3d 983, 1004 [254 Cal.Rptr. 786, 766 P.2d 1] [court gave "full recognition of both the statutory and constitutional bases of [De Lance]"]; Donaldson, supra, 35 Cal.3d at p. 37 [phr. opn. of Broussard, J.] ["De Lance was clearly not a simple application of the statutory language"]; id., at p. 41, fn. 1 (dis. opn. of Reynoso, J.) [issue implicates "constitutional right of privacy"]).

We thus decided in De Lance that the 1975 statutory amendments "established a policy that prisoners retain the rights of free persons, including the right of privacy, except to the extent that restrictions are necessary to ensure *1008 the security of the prison and the protection of the public." (De Lance, supra, 31 Cal.3d at p. 868.)

FN13 We have also recognized that the decision shifted the law: "Under settled federal precedent and under the California decisions prior to De Lance ... the secret monitoring and recording of unprivileged conversations in prisons, jails, and police stations did not constitute an unlawful search." (Donaldson, supra, 35 Cal.3d at p. 27.)

FN13 End. If prisoners enjoyed the same degree of legal protection as free persons, it is not evident that the surveillance was unlawful. In People v. Kauanagna (1977) 70 Cal.App.3d 283 [138 Cal.Rptr. 651], the Court of Appeal found there was no privacy violation where police, suspecting unlawful activity in a boardinghouse room, entered, with the building manager's permission, the vacant room adjacent to the suspected crime site and overheard incriminating evidence. "We do not believe ... the Californians ... right to privacy ... governed by the same standards recognized in criminal cases. [¶] Thus, the California statute is applicable to the situation here, and we conclude that the police did not violate the privacy rights of the defendant." (Id. at p. 288.)

E. Restoring Harrell

Just as the establishment of Procurer's strict
standard led to the abolition of the *Harrell* standard, the abandonment of *Procurer* led to Harrell's restoration. In *Turner*, supra, 482 U.S. 78, the United States Supreme Court formally determined the question reserved in *Procurer* by concluding that case protected the First Amendment rights of only the civilians with whom the inmates were corresponding. The rights of prisoners enjoyed less stringent protection; "when a prison regulation impinges on inmates' constitutional rights, the regulation is valid if it is reasonably related to legitimate penological interests." (*Turner*, at p. 89 [107 S.Ct. at p. 2261]). The state Legislature adopted this standard in its 1994 amendment to section 2600, which now reads, "A person sentenced to imprisonment in a prison state may ... be deprived of such rights, and only such rights, as is reasonably related to legitimate penological interests."

The amendment reflected the Legislature's desire to repeal the expansive protections afforded California inmates and replace them with the more limited protections available under federal law as described in *Turner*, supra, 482 U.S. 78. In *Thompson v. Department of Corrections* (2001) 25 Cal.4th 117, 130 [105 Cal.Rptr.2d 46, 18 P.3d 1198], we observed the 1994 amendment abrogated: the standard we had followed in *In re Arias* (1986) 42 Cal.3d 667 [230 Cal.Rptr. 505, 725 P.2d 664]. *Thompson* recognized prison restrictions on inmate liberties that might have been invalid prior to 1994 could now be valid. (*Thompson*, at pp. 129-130 [restriction on practice of religion that might have been invalid under pre-1994 standard was valid under new law].) We held the monitoring of inmates' conversations with visitors to be another such regulation that has become valid after the 1994 amendment. *1009*

Construing the "legitimate penological objectives" in *Harrell*, supra, 2 Cal.3d at page 702, and "legitimate penological interests" in the current section 2600 and finding them comparable phrases, we conclude the current standard is less restrictive than the *Harrell* test. Our former standard permitted restrictions on inmates' activities "only in accordance" (*Harrell*, at p. 702) with the proper goals, whereas the current standard permits such restrictions whenever they are "reasonably related" to the goals (*Turner*, supra, 482 U.S. at p. 89 [107 S.Ct. at p. 2261]). We therefore conclude the Legislature, in restoring the legitimate penological objectives/interests standard of *Harrell*, intended to restore the former law regarding inmates' rights. (2) (See fn. 14.) Any restrictions on inmates' rights that were lawful prior to *De Lance*, a fortiori, will be lawful under the current test. [FN14] Because the current standard was operative during the surveillance challenged below, and such surveillance was lawful prior to *De Lance*, we find it was lawful in this case, and therefore not misconduct. [FN15]

---

**FN14** Our decision today allows police officers to monitor conversations in jail as they may monitor conversations in police cars, in accordance with *People v. Crowson* (1983) 33 Cal.3d 623 [190 Cal.Rptr. 165, 660 P.2d 389]. There is no longer a distinction between the two locations regarding an individual's reasonable expectations of privacy in her communications. (See *People v. Califano* (1970) 5 Cal.App.3d 476, 481-482 [85 Cal.Rptr. 292]; *People v. Chandler* (1958) 262 Cal.App.2d 350, 356 [68 Cal.Rptr. 645].)

**FN15** In 1996, the Legislature further distanced statutory law from *De Lance* by repealing the section 2601; subdivision (d), right to visits. (Stats. 1996, ch. 132, § 1.) The Legislature has thus completely "delete[d] the language quoted", in *De Lance*, (6 Wilkin & Epstein, Cal. Criminal Law (3d, ed. 2000) Illegally Obtains Evidence, § 352, p. 1037.)


**FN16** Defendant cites the mapposite case of *United States v. Cohen* (2d Cir. 1986) 796 F.2d 20,
where the Second Circuit Court of Appeals suppressed documents discovered during a search of the defendant's cell conducted to gather evidence. Because Cohen was decided before Turner, supra, 482 U.S. 78, the Second Circuit followed the "rule that when a prison restriction infringes upon a specific constitutional guarantee, it should be evaluated in light of institutional security." (Cohen, at p. 22.) It is far from certain that the Second Circuit Court of Appeals would have reached the same result after Turner announced its more deferential test. In any event, because the evidence seized was paper located in the inmate's cell, rather than statements made during conversations with visitors, it is factually distinguishable.

Similarly inapposite is defendant's reference to Ferguson v. Charleston (2001) 532 U.S. 67 [121 S.Ct. 1281, 149 L.Ed.2d 205], for the proposition that the instant investigative purpose rendered the monitoring unlawful. The Ferguson court invalidated hospital personnel's searching and seizing patients' urine to analyze for evidence of criminal activity. The court found the search and seizure served only general law enforcement purposes, and not "special needs," which would justify dispensing with traditional Fourth Amendment protections. (Id. at p. 77 [121 S.Ct. at p. 1288].) By contrast, the constant monitoring implicates no Fourth Amendment protections. The interest of public safety is so compelling that it may be relevant when determining the scope of constitutional protections (see, e.g., New York v. Quares (1984) 467 U.S. 649 [104 S.Ct. 2626, 81 L.Ed.2d 550], but this hardly means police must show a public safety purpose to investigate crime where no constitutional prohibition exists.

Conclusion

We therefore conclude that De Lancei, supra, 31 Cal.3d 865, no longer correctly states California law regarding inmate rights. Following the 1994 amendment to section 2600, California law now permits law enforcement officers to monitor and record unprivileged communications between inmates and their visitors to gather evidence of crime. Accordingly, we affirm the judgment of the Court of Appeal.


KENNARD, J.

I concur in the majority's result, but would analyze the matter differently.

Our decision in De Lancei v. Superior Court (1982) 31 Cal.3d 865 [183 Cal.Rptr. 866, 647 P.2d 142], held that surreptitious recording of conversations between an inmate in jail awaiting trial and his visitors, unless justified by security concerns, violated the inmate's right of privacy. De Lancei was based on Penal Code section 2600, which from 1975 until 1995 provided: "A person sentenced to imprisonment ... may, during any such period of confinement, be deprived of such rights, and only such rights, as is necessary in order to provide for the reasonable security of the institution in which he is confined and for the reasonable protection of the public." (Stats. 1975, ch. 1175, § 3, p. 2877.) De Lancei held that pretrial detainees enjoyed at least the same rights as convicted inmates, and observed that recording conversations between inmates and visitors would violate section 2600 if the recordings were "undertaken for the purpose of gathering evidence for use in criminal proceedings, rather than to maintain the security of the jail." (De Lancei, at p. 877.)

The 1994 Legislature, however, amended section 2600 to provide: "As it does today, ... A person sentenced to imprisonment in a state prison may ... *1011 be deprived of such rights, and only such rights, as is reasonably related to legitimate penological interests." In Thompson v. Department of Corrections (2001) 25 Cal.4th 117, 130 [105 Cal.Rptr.2d 46, 18 P.3d 1198], we concluded that this amendment adopted the view of the United States Supreme Court in Turner v. Safely (1987) 482 U.S. 78, [107 S.Ct. 2254, 96 L.Ed.2d 64], under which the monitoring of inmate conversations with visitors to gather evidence against the inmate is justified as reasonably related to a legitimate penological goal. As interpreted in Thompson, the 1994 amendment effectively abrogated this court's holding in De Lancei.

Consequently, there is no need for the majority to discuss pre-De Lancei California decisions, to determine whether or not De Lancei was correctly decided in the first place, or to consider whether the 1994 Legislature intended not only to adopt the standard of Turner v. Safely, supra, 482 U.S. 78, but also to resurrect In re Harrell (1970) 2 Cal.3d 675 [87 Cal.Rptr. 504, 470 P.2d 640]. The majority's sweeping assertion that "[a]ny restrictions on inmates' rights that were lawful prior to "De
Lancie ... will be lawful under the current test (maj. opn., ante, at p. 1009) remains to be tested when the courts examine specific restrictions.

Law enforcement authorities in California are required to comply with state restrictions on the gathering of evidence, even when those restrictions cannot be enforced by excluding that evidence from admission. Thus, the prosecution here took a considerable risk in instituting a surveillance practice this court had condemned in De Lancie at a time when no court decisions had construed the 1994 amendment to Penal Code section 2600. But because the majority concludes that the 1994 amendment does support the prosecution’s action and effectively abrogated the holding in De Lancie, it correctly affirms the Court of Appeal decision rejecting the imposition of sanctions on the prosecution.

WERDEGAR, J., Concurring.

I agree with the majority that the monitoring and recording of defendant’s personal visits did not violate California law, despite our decision in De Lancie v. Superior Court (1982) 31 Cal.3d 865 [183 Cal.Rptr. 866, 647 P.2d 142] (De Lancie). In my view, however, this is true not because the holding of De Lancie has been abrogated by intervening amendments to Penal Code section 2600, [FN1] but because De Lancie was erroneously decided.

FN1 All further statutory references are to the Penal Code.

In De Lancie, this court assumed that an incarcerated person had a reasonable expectation of privacy in his or her conversations, creating a privacy right upon which jail officials could, under section 2600, infringe *1012 only as necessary for institutional security. (De Lancie, supra, 31 Cal.3d at pp. 873-876.) Our error, as the dissenting justices explained, was in assuming that either the common law or constitutional right to conversational privacy persisted when a person entered prison or jail and became subject to the pervasive official surveillance that traditionally characterizes those environments. (See id. at p. 881 (dis. opn. of Richardson, J.) ["A man detained in jail cannot reasonably expect to enjoy the privacy afforded to a person in free society. His lack of privacy is a necessary adjunct to his imprisonment"] ; id. at p. 882 (dis. opn. of Mosk, J.) ["The concept of one purporting to enjoy privacy while he is under legally authorized supervision would appear to be a monumental anomaly"]).

Though the court’s opinion in De Lancie displays some confusion on this point, that the versions of sections 2600 and 2601 then in force did not confer on prisoners a right of conversational privacy is clear; at most the statutes limited the extent to which jail officials could curtail an otherwise existing right. Section 2600 simply provided that prisoners could be “deprived of such rights, and only such rights,” as was necessary for institutional security. (De Lancie, supra, 31 Cal.3d at p. 870.) Of course, no deprivation can occur if no right exists. Section 2601 guaranteed certain enumerated rights, including personal visits, but these did not include the right to conduct such visits, or other jailhouse conversations, in privacy. (De Lancie, at p. 870.)

As sections 2600 and 2601 did not themselves confer a right of privacy in jailhouse conversations, and as the court did not cite any other statutory basis, the right of privacy the De Lancie majority recognized could only have derived from the common law, the California Constitution’s privacy guarantee (art. I, § 1), or the constitutional prohibitions against unreasonable searches (U.S. Const., 4th Amend.; Cal. Const., art. I, § 13). But all these sources require as a predicate to establishing an invasion of privacy or unreasonable search that the person had an objectively reasonable expectation of privacy in the invaded place, conversation or data source. (See Shulman v. Group W Productions, Inc. (1998) 18 Cal.4th 200, 232 [74 Cal.Rptr.2d 843, 955 P.2d 469]; Hill v. National Collegiate Athletic Assn. (1994) 7 Cal.4th 1, 36-37 [26 Cal.Rptr.2d 834, 865 P.2d 633]; Donaldson v. Superior Court (1983) 35 Cal.3d 24, 28-30 [196 Cal.Rptr. 704, 672 P.2d 110].) Courts have generally found no reasonable expectation of privacy in jailhouse conversations for purposes of search and seizure law (see Donaldson v. Superior Court, at pp. 30-34; U.S. v. Peoples (8th Cir. 2001) 250 F.3d 630, 636-637), and this court itself had, prior to De Lancie, recognized the general rule that “an inmate of a jail or prison has no reasonable expectation of privacy” in conversations while incarcerated (North v. Superior Court *1013 (1972) 8 Cal.3d 301, 311 [104 Cal.Rptr. 833, 502 P.2d 1305, 57 A.L.R.3d 155]).
Nevertheless, the *De Lancie* majority rejected the rule stated in *North v. Superior Court*, *supra*, and other cases, because in its view "[t]o deny a right of privacy on the ground that inmates, disabused by prior decisions, have lost their normal expectation of privacy would defeat the purposes of the statutes."

(*De Lancie*, *supra*, 31 Cal.3d at p. 876.) This reasoning simply begged the question. The effect of prior decisions on prisoners' subjective expectations aside, no objectively reasonable expectation of conversational privacy can be maintained in prison or jail, because of the pervasive and constant monitoring to which incarcerated persons are subject. The *De Lancie* majority, unlike the dissenters, closed its eyes to that fundamental fact. In so doing, it erred.

For these reasons, I concur in the judgment.

MORENO, J., Concurring

I agree with the majority that our decision in *De Lancie v. Superior Court* (1982) 31 Cal.3d 865 [183 Cal.Rptr. 866, 647 P.2d 142]. (*De Lancie*) was superseded by the 1994 amendment to Penal Code section 2600 such that, subject to Penal Code section 636. [FN1] "California law now permits law enforcement officers to monitor and record unprivileged communications between inmates and their visitors to gather evidence of crime." (Maj. opn., ante, at p. 1010.) In this case, however, the Alameda County prosecutor, without a warrant, asked the Santa Rita jail authorities to monitor and record defendant's in-house jail conversations and her outbound telephone calls. I write separately to underscore that federal law, specifically, title III of federal Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. §§ 2510-2520), the Act, still restricts the warrantless monitoring [FN2] of an inmate's outbound telephone calls.

*FN1* Penal Code section 636, subdivision (a), makes it a felony to eavesdrop on, or secretly record, a detaine's or prisoner's conversation with his or her "attorney, religious adviser, or licensed physician."

*FN2* Where authorities have the right to monitor, they also have the right to record. (See, e.g., *People v. Murphy* (1972) 8 Cal.3d 349, 360 [105 Cal.Rptr. 138, 503 P.2d 594].)

In *People v. Otto* (1992) 2 Cal.4th 1088 [9 Cal.Rptr.2d 596, 831 P.2d 1178], we recognized that the Act governs wiretapping violations in California. We stated: "The purpose of the [Act] ... was effectively to prohibit ... all interceptions of oral and wire communications, except those specifically provided for in the Act ..." (*Otto*, *supra*, at p. 1100, quoting *United States v. Giordano* (1974) 416 U.S. 505, 514 [94 S.Ct. 1820, 1826, 40 *1014 L.Ed.2d 341].) The Act defines a "wire communication" as "any aural transfer ... by the aid of wire, cable, or other like connection between the point of origin and the point of reception ... furnished or operated by a [common carrier] ...." (18 U.S.C. § 2510(1)). As common carriers operate outbound telephones, calls over such telephones are "wire communications." Internal jail phones, on the other hand, are not part of any public telephone system and are not furnished by a common carrier. As such, they are not covered by the Act. (See, e.g., *People v. Santos* (1972) 26 Cal.App.3d 391, 401-402 [102 Cal.Rptr. 678].)

The Act requires that a judicially authorized warrant be obtained before wiretapping can take place. (18 U.S.C. § 2518.) There are two exceptions to the warrant requirement: (1) where the interception is "by an investigative or law enforcement officer in the ordinary course of his duties" (18 U.S.C. § 2510(5)(a)(ii)); or (2) where a person acting under color of law "wireraps, and one party to the communication has given prior consent. (18 U.S.C. § 2511(2)(c).) Where the Act is violated, the remedy is suppression of the intercepted communication. (18 U.S.C. § 2515.)

In the seminal case of *United States v. Paul* (6th Cir. 1980) 614 F.2d 115, 61 A.L.R.Fed. 816 (*Paul*), the government took the broad view that the Act did not apply to the secret recording of outbound telephone calls originating from prison. (Id. at p. 116.) The *Paul* court rejected this argument and held that the Act did apply, but found that the prison wiretap was permissible under 18 United States Code section 2510(5)(a)(ii), the Act's "ordinary course of duties" exception, because (1) the monitoring was done pursuant to a policy statement issued by the Federal Bureau of Prisons; and (2) posted telephone rules gave the inmates "reasonable notice" that such monitoring might occur. (Paul, 3826 -
In *U.S. v. Sababu* (7th Cir. 1989) 891 F.2d 1308, 1328-1329, the court found the ordinary course of duties exception applied where (1) the monitoring was conducted pursuant to an established prison policy; (2) monitoring notices were posted over each outbound telephone in English and Spanish; and (3) during orientation, the inmates were told that their outbound telephone conversations were subject to monitoring.

The federal courts have also found, under similar facts, that jailhouse wiretapping falls within the "implied consent" theory. For example, in *U.S. v. Lloyd* (2d Cir. 1987) 831 F.2d 373, 378-379, the court found "implied consent" where, (1) the prisoner attended a lecture that outlined the prison's monitoring policy; (2) he received a copy of a handbook that stated that outbound telephone calls would be monitored; and (3) monitoring notices, in English and Spanish, were placed on each outbound telephone.

In *U.S. v. Van Poyck* (9th Cir. 1997) 77 F.3d 285, 291-292, the court found "implied consent" where (1) the defendant signed a form that warned him of the prison's monitoring and taping policy; (2) he was given a prison booklet explaining possible recording; and (3) monitoring notices were posted by the outbound telephones.

It thus appears that the warrantless monitoring of an inmate's outbound telephone calls is prohibited by the Act, unless the inmate is given meaningful notice, such as by a signed acknowledgement form, a monitoring notice posted by the outbound telephone, or a recorded warning that is heard by the inmate through the telephone receiver, prior to his or her making the outbound telephone call.

II

In the case at bar, from March 26, 1996 through June 30, 1996, the Alameda County prosecutor requested that jail officials at the Santa Rita jail secretly record all of defendant's outbound phone calls to her friend, Ann Argabrite, and her brother, Philip Loyd. The prosecutor also requested that all of defendant's in-house nonattorney jail conversations be recorded. The prosecutor made these requests without the benefit of a warrant. There were no warning signs in the outbound telephone area indicating that calls might be recorded. While the outbound phone system was configured to play a taped warning, the system was malfunctioning in March and April of 1996 and became operative sometime in June of 1996. It was established in the trial court that, upon arrival, each inmate was given a copy of jail rules and regulations, but it was unknown whether Loyd actually received a pamphlet that contained a warning about the monitoring policy. However, the pamphlet typically contained such a warning. Finally, jail officials operated the telephone monitoring system according to an established monitoring policy.

The Act was given short shrift at the trial court level. As stated by the Court of Appeal, "defendant placed no emphasis on it and never specifically informed the trial court that it might supply authorization to exclude the tapes." A review of the briefs made no factual findings as to specific dates that defendant's outbound calls were secretly recorded. Nor did the trial court determine if any particular recording was a product of an in-house jail conversation or an outbound telephone call. I therefore agree with the Court of Appeal that the Act was not properly raised.

III

In *People v. Riel* (2000) 22 Cal.4th 1153 [96 Cal.Rptr.2d 1, 998 P.2d 969], we refused to exclude a secretly recorded in-house jail conversation, obtained in violation of *De Lancee*, under the truth-in-evidence provision (Cal. Const., art. I, § 28, subd. (d)), because "federal law [did] not bar its admission." *(Riel, supra, at p. 1184, quoting People v. Hines* (1997) 15 Cal.4th 997, 1043 [64 Cal.Rptr.2d 594, 938 P.2d 388].) A question left open in *Riel*, and resolved here, is whether a prosecutor's warrantless request for in-house jail monitoring constitutes prosecutorial misconduct. As noted, where this request is limited to the secret monitoring of internal jail phones, the request is appropriate. Where a prosecutor requests the monitoring of outbound telephone calls, however, any monitoring must comply with the provisions of the Act. Prosecutors who request such monitoring...
have, at a minimum, an ethical obligation to ensure that such monitoring is in compliance with the Act. The demise of De Lance does not signal a death knell for the protections afforded under federal law.

Kennard, J., concurred. *1017

THE PEOPLE, Plaintiff and Respondent, v. CHRISTINE LOYD, Defendant and Appellant.

END OF DOCUMENT
Client Identifier: SARIA
Date of Request: 01/09/2003
Current Database is CA-CS
127 Cal.Rptr.2d 203
(Cite as: 163 Cal.App.4th 853, 127 Cal.Rptr.2d 203)

Court of Appeal, First District, Division 5,
California.

The PEOPLE, Plaintiff and Respondent,
v.
Tshombe KELLEY, Defendant and Appellant.

No. A093862.

Certified for Partial Publication. [FN*]

FN* Pursuant to California Rules of Court, rule 976(b)(1) and (3) the court orders publication of the introductory paragraph, Background, part III of the Discussion, and the Disposition of its opinion in People v. Kelley, A093862.

Rehearing Denied Nov. 18, 2002.

Defendant was convicted in the Superior Court, Alameda County, No. CI139184, Vernon Nakahara, J., of murder. Defendant appealed. The Court of Appeal, Gemello, J., held that wiretap of defendant's prison telephone conversations was not unlawful.

Affirmed.

West Headnotes

[1] Telecommunications @=493
372k493

Title III of the Omnibus Crime Control and Safe Streets Act protects an individual from all forms of wiretapping except when the statute specifically provides otherwise; the protections apply to prisoners and prison monitoring. 18 U.S.C.A. § 2511(2)(c).

[2] Telecommunications @=495
372k495

The legislative history of Title III of the Omnibus Crime Control and Safe Streets Act, which protects an individual from all forms of wiretapping except when the statute specifically provides otherwise, shows that Congress intended the consent requirement to be construed broadly 18 U.S.C.A. § 2510 et seq.

[3] Telecommunications @=495
372k495

Wiretap of defendant's telephone conversations while defendant was in prison was not unlawful; defendant had meaningful notice that telephone calls over the prison phones were subject to monitoring, his decision to engage in conversations over those phones constituted implied consent to that monitoring and made any wiretap lawful, and no judicial approval was required; as defendant "consented" to the recording of his conversations. 18 U.S.C.A. § 2511(2)(c); West's Ann. Cal.Penal Code §§ 629.50, 631(a).


Matthew Zwerling and J. Bradley O'Connell, under appointments by the Court of Appeal, for Defendant and Appellant.

*855 GEMELLO, J.

Tshombe Kelley appeals his conviction for first degree murder and sentence of 52 years to life, raising a variety of issues. Only one has merit: we agree that the prosecution should not have been permitted to cross-examine Kelley concerning prior unproven crimes. However, because any error in this regard was harmless in light of the considerable evidence against Kelley, we affirm the judgment in its entirety. [FN1]

FN1. Kelley has also filed a petition for writ of habeas corpus (A093862) related to this appeal. By separate order filed on this same date, we deny the petition.

BACKGROUND

On May 21, 2000, at 6:31 p.m., a 911 operator received a call that a man had been shot in the 4100 block of Mera Avenue in Oakland. The call came from Kelley's next-door neighbors, who heard shots coming from Kelley's house at 4126 Mera. While
the husband was on the phone, the wife saw the victim, Aaron Stewart, slump over, walking up to a neighbor's porch. She went out to Stewart. He was unable to respond to questions. He died from multiple gunshot wounds in the back. The neighbors saw no one else in the area.

Another neighbor heard shots. She awakened the father of her children. He saw Stewart slump outside their house, went outside, and saw Kelley outside in his yard. When he asked what happened, Kelley replied, "Dude tried to rob me. Give dude back his keys," and held out a set of keys.

Police arrived within two minutes. A few minutes later, an officer saw Kelley, sweating, through the screen door of Kelley's house. When the officer asked Kelley to talk to him, Kelley began to shake and announced, "I didn't shoot anybody."

Forensic tests found blood inside Kelley's gate. The blood was consistent with Stewart's. A bullet hole in the gate indicated that a shot had been fired from Kelley's doorway or porch. Kelley's right hand tested positive for gunshot residue, though in a quantity insufficient to establish that he had recently fired a gun. Neither the murder weapon nor any spent shells were found.

*856 The three adults at 4126 Mera were Kelley, his girlfriend Corrie Tridente, and Tridente's cousin, Cassandra Bugnatto. They were detained and questioned separately Bugnatto, who was away at a laundromat during the shooting, said that Stewart and Kelley had had a falling out over an affair between Tridente and Stewart. After initially denying that she knew Stewart, Tridente admitted that she had had an affair with Stewart. She said that when Stewart came by, Kelley got a gun and went out to meet him. She heard yelling and then gunshots. Kelley refused to speak with police without an attorney present. Early on the morning of the 22nd, he was charged with murder.

In September 2000, shortly before trial, the prosecution asked for Kelley's outbound calls from prison to be taped. Based on these tapes, the prosecution obtained a search warrant for Kelley's prison cell and Tridente's residence, which at the time of trial was her grandmother's home. The search yielded numerous letters between Kelley, Tridente, and others that formed a central part of the prosecution's case. In these letters, Kelley coached Tridente on what actions and testimony would be favorable and suggested testimony for Bugnatto. In an October 3 letter, he asked Tridente to refuse to testify, notwithstanding any court order, in the hope of suppressing her May 21 taped statements.

At trial, the prosecution introduced testimony from numerous witnesses that Tridente and Stewart had had an affair in 1999, and that Kelley threatened to harm or kill Stewart as a result. Stewart and Kelley were one-time friends; at some point after the affair, they partially reconciled.

In the spring of 2000, Kelley bought a car from Stewart. When it broke down **205 shortly thereafter, Kelley held off on paying Stewart. In late April, according to prosecution witnesses, Kelley went to Stewart's house, argued with Stewart, fired a gun in the air, and left. Kelley returned that day and aimed a gun at Stewart; according to some witnesses, the gun jammed, while according to another, it was not loaded and Kelley was just trying to scare Stewart. Kelley made further threats on Stewart's life.

On May 21, the day of the shooting, Bugnatto, a friend of both Stewart and Kelley, was babysitting Stewart's son at Kelley's house. Another mutual friend of Stewart and Kelley who was with Stewart that day, David Maldonado, testified that Stewart received a call to come pick up his son from Kelley's apartment. Stewart used Maldonado's car. Maldonado called Kelley immediately after Stewart left. Kelley asked whether Maldonado was with Stewart; Maldonado said no, implying that Stewart was coming alone.

Tridente was unwilling to testify and did so only after the court granted her immunity and ordered her to testify. She repudiated her May 21 statements.

*857 Kelley testified in his own defense. He denied that he shot Stewart. Though he knew about the affair, he denied any lasting problems with Stewart. On the evening of the shooting, he and Tridente were at home when they heard shots. Kelley saw what looked like a white male go past his window. He went outside, recognized Maldonado's car, and thought that someone must have tried to rob Maldonado. He said to his neighbor, not "Dude tried to rob me," but "
Someone tried to rob him." Only later, when he saw the body being taken away, did he realize that it was Stewart who had been shot.

A jury convicted Kelley of first degree murder (Pen.Code, § 187) and personal use of a firearm resulting in great bodily injury or death (Pen.Code, § 12022.53, subs.(c) and (d)), based on the Stewart shooting, as well as willfully discharging a firearm in a 'grossly negligent manner (Pen.Code, § 246.3), based on the late April incident where Kelley fired a gun in the air at Stewart's house. The court sentenced Kelley to 52 years to life.

Kelley has timely appealed.

I-II. [FN**]

FN** See footnote *, ante.

III. The Prosecution's Wiretap of Kelley's Jailhouse Conversations Was Legal

The prosecution recorded Kelley's jailhouse telephone conversations and introduced portions of the transcripts, as well as evidence seized based on those conversations. Kelley challenges the wiretap under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 United States Code section 2510 et seq. ("Title III") and state law. We review these issues de novo. (U.S. v. Van Poyck (9th Cir.1996) 77 F.3d 285, 291.) We find no violation of either federal or state law.

[1] With certain limited exceptions, Title III prohibits the unauthorized interception of "any wire, oral, or electronic communication." (18 U.S.C. § 2511, subd. (l)(a).) Thus, "[i]t protects an individual from all forms of wiretapping except when the statute specifically provides otherwise." (Abraham v. County of Greenville, S.C. (4th Cir.2001) 237 F.3d 386, 389.) Those protections apply to prisoners and prison monitoring. (See, e.g., U.S. v. Amen*858 (2d Cir.1987) 831 F.2d 373, 378.) Therefore, the recordings of Kelley were **266 obtained legally only if one of the statutory exceptions to the prohibition applies. The People argue that two of the specified exceptions, the consent and law enforcement exceptions, render its use of the recordings proper in this case. Because we agree that the consent exception applies, we need not address the law enforcement exception.

[2] Under Title III, "it shall not be unlawful ... for a person acting under color of law to address a wire, oral, or electronic communication, where ... one of the parties to the communication has given prior consent to such interception." (18 U.S.C. § 2511, subd. (2)(c).) "The legislative history of [Title III] shows that Congress intended the consent requirement to be construed broadly." (Amen, supra, 831 F.2d at p. 378; see S.Rep. No. 1097, 90th Cong., 2d Sess., reprinted in 1968 U.S.C.C.A.N. 2112, 2182.) Consistent with this intent, every federal circuit court to address the question has concluded that a prisoner who, while on notice that his telephone conversation is subject to tapping, proceeds with the conversation, has given implied consent to that tapping. (U.S. v. Footman (1st Cir.2000) 215 F.3d 145, 155; U.S. v. Workman (2d Cir.1996) 80 F.3d 688, 693-694; U.S. v. Horr (8th Cir.1992) 963 F.2d 1124, 1125-1126; Van Poyck, supra, 77 F.3d at p. 292; but see U.S. v. Daniels (7th Cir.1990) 902 F.2d 1238, 1244-1245 [criticizing other courts' broad views of consent but deciding case on another ground].)

Our Supreme Court's recent decision in People v. Loyd (2002) 27 Cal.4th 997, 119 Cal.Rptr.2d 360, 45 P.3d 296 demonstrates that at least two members of that court would agree with the views of these federal courts. While the majority found it unnecessary to reach the issue, Justice Moreno, joined by Justice Kennard, spelled out his agreement with the consensus interpretation of the circumstances sufficient to find implied consent by prisoners. (Id. at pp. 1014-1015, 119 Cal.Rptr.2d 360, 45 P.3d 296 [conc. op. of Moreno, J.].) We agree as well. So long as a prisoner is given meaningful notice that his telephone calls over prison phones are subject to monitoring, his decision to engage in conversations over those phones constitutes implied consent to that monitoring and takes any wiretap outside the prohibitions of Title III.

Kelley relies on two passages from earlier California Supreme Court decisions to argue that that court would take a different view of Title III than the federal courts. (People v. Otto (1992) 2 Cal.4th 1088, 1098-1099, fn. 7, 9 Cal.Rptr.2d 596, 831 P.2d 1178; Halpin v. Superior Court (1972) 6
Kelley's monitoring, he had notice that InscaJls were subject to notice previously found sufficient to hold that a prisoner has impliedly consented to monitoring. (See Amen, supra, 831 F.2d at p. 379; Workman, supra, 80 F.3d at p. 693; Van Poyk, supra, 77 F.3d at p. 292; Hogg, supra, 963 F.2d at p. 1126.) Because Kelley had notice that his calls were subject to monitoring, he consented when he used the prison's phone system.

It is true that this rule presents prisoners with "a choice between unattractive options," limiting their contact with the outside world or submitting to government eavesdropping. (Langton v. Hogan (1st Cir.1995) 71 F.3d 930, 936.) However, there is no reason to believe Congress intended to draw the statute so narrowly as to exclude such prisoner choices from the notion of consent. (Footman, supra, 215 F.3d at p. 155.) The use of prison telephones is a privilege, not a right.

With respect to state law, our Supreme Court recently held that a prosecutor does not commit misconduct when he seeks the surreptitious recording of conversations between an imprisoned defendant and third parties, as the deputy district attorney did here. (Loyd, supra, 27 Cal.4th 997, 119 Cal.Rptr.2d 360, 45 P.3d 296.) Twenty years earlier, the same court held that such actions constituted misconduct. (DeLancey v. Superior Court (1982) 31 Cal.3d 865, 183 Cal.Rptr. 647, 629.50.) However, Loyd concluded that intervening statutory amendments have abrogated DeLancey. (Loyd, supra, 27 Cal.4th at p. 1010, 119 Cal.Rptr.2d 360, 45 P.3d 296.)

Kelley concedes that Loyd disposes of his state law challenge to the wiretapping based on DeLancey. However, he raises a second state law challenge based on Penal Code section 629.50. We find no violation of that *860 statute either. Section 629.50 governs applications for judicial approval of wiretapping. No such approval was required here. California's wiretapping statutes, like Title III, do not apply to the monitoring and recording of conversations where one party consents. (Pen.Code, § 631, subd. (a), prohibiting only "unauthorized" wiretaps; People v. Canard (1967) 257 Cal.App.2d 444, 463-464, 65 Cal.Rptr. 15.) Because Kelley consented to have his conversations monitored, the deputy district attorney did not need to seek judicial approval, and section 629.50 is inapplicable. The admission of tapes of Kelley's conversations, as well as the fruits of those tapes, was proper.

IV. The Prosecution's Questioning About Unproven Prior Crimes Was Harmless Beyond a Reasonable Doubt in Light of All the Evidence [FN***]

FN*** See footnote *, ante.

DISPOSITION

The judgment is affirmed.

We concur. JONES, P.J., and STEVENS, J.


END OF DOCUMENT

Copr. © West 2003 No Claim to Orig. U.S. Govt. Works

- 3833 -
ACLU asks California to monitor FBI spying

Published 12:20 p.m. PDT Saturday, July 6, 2002

SAN FRANCISCO (AP) - The American Civil Liberties Union has urged state Attorney General Bill Lockyer to prevent FBI spying on political dissidents after recent revelations the agency had done so in the past.

In an open letter to Lockyer the ACLU's three state chapters urged Lockyer to enforce the state's right to privacy, adopted by voters in 1972:

The ACLU cited a recent story by the San Francisco Chronicle which detailed that the FBI had spied on student activists at the University of California, Berkeley in the 1960s.

U.S. Attorney General John Ashcroft announced guidelines May 30 allowing FBI agents to conduct surveillance in places that are open to the public, without evidence that those being watched have committed or are planning to commit crimes.

"California has drawn a line with respect to privacy, political and associational rights that government must not cross even with the best of intentions," the ACLU letter said. "Yet, some of the intelligence practices now openly encouraged by the new federal guidelines cross that long-standing state line."

The guidelines repealed rules imposed by President Gerald Ford that allowed FBI surveillance only during criminal investigations and after evidence of wrongdoing. President Bush claimed that those restrictions gave terrorists and advantage and pledged that the new FBI powers would not stifle speech or dissent.

The ACLU letter asked Lockyer to advise state and...
local police that they were still bound by California's privacy law even when working with federal agents. Although the FBI is not bound by state laws, Lockyer should still "strongly encourage" federal agents to abide by the state's privacy laws when collecting information in the state.

Lockyer's office promised a prompt reply and said it was complying with state law in its post-Sept. 11 anti-terrorism projects, including the establishment of an information-sharing central database accessible to local, state and federal law enforcement.

"We have no intention of trampling Californians' privacy," spokeswoman Hallye Jordan told the San Francisco Chronicle.

The database includes only the names of those suspected of terrorism-related crimes or who are being investigated for such crimes based on evidence, Jordan said.

Information from: San Francisco Chronicle
MEMORANDUM FOR THE HEADS AND INSPECTORS GENERAL OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: THE ATTORNEY GENERAL

SUBJECT: Procedures for Lawful, Warrantless Monitoring of Verbal Communications

By Memorandum dated October 16, 1972, the Attorney General directed all federal departments and agencies to obtain Department of Justice authorization before intercepting verbal communications without the consent of all parties to the communication. This directive was clarified and continued in force by the Attorney General’s Memorandum of September 22, 1980, to Heads and Inspectors General of Executive Departments and Agencies. It was then superseded, with new authorization procedures and relevant rules and guidelines, including limitations on the types of investigations requiring prior written approval by the Department of Justice, in the Attorney General’s Memorandum of November 7, 1983.1

The Attorney General’s Memorandum of January 20, 1998, superseded the aforementioned directives. It continued most of the authorization procedures established in the November 7, 1983, Memorandum, but reduced the sensitive circumstances under which prior written approval of senior officials of the Department of Justice’s Criminal Division is required. At the same time, it continued to require oral authorization from Department of Justice attorneys, ordinarily local Assistant United States Attorneys, before the initiation of the use of consensual monitoring in all investigations not requiring prior written approval. In addition, that Memorandum reduced and eventually eliminated the reporting requirement imposed on departments and agencies. These changes reflected the results of the exercise of the Department’s review function over many years, which showed that the departments and agencies had uniformly been applying the required procedures with great care, consistency, and good judgment, and that the number of requests for consensual monitoring that were not approved had been negligible.

1As in all of the prior memoranda except for the one dated October 16, 1972, this memorandum only applies to the consensual monitoring of oral, nonwire communications, as discussed below. “Verbal” communications will hereinafter be referred to as oral.
This Memorandum updates and in some limited respects modifies the Memorandum of January 20, 1998. The changes are as follows:

First, Parts III.A.(8) and V. of the January 20, 1998, Memorandum required concurrence or authorization for consensual monitoring by the United States Attorney, an Assistant United States Attorney, or the previously designated Department of Justice attorney responsible for a particular investigation (for short, a "trial attorney"). This Memorandum provides instead that a trial attorney must advise that the monitoring is legal and appropriate. This continues to limit monitoring to cases in which an appropriate attorney agrees to the monitoring, but makes it clear that this function does not establish a supervisory role or require any involvement by the attorney in the conduct of the monitoring. In addition, for cases in which this advice cannot be obtained from a trial attorney for reasons unrelated to the legality or propriety of the monitoring, this Memorandum provides a fallback procedure to obtain the required advice from a designated attorney of the Criminal Division of the Department of Justice. Where there is an issue as to whether providing the advice would be consistent with applicable attorney conduct rules, the trial attorney or the designated Criminal Division attorney should consult with the Department's Professional Responsibility Advisory Office.

Second, Part V. of the Memorandum of January 20, 1998, required that an agency head or his or her designee give oral authorization for consensual monitoring, and stated that "[a]ny designee should be a high-ranking supervisory official at headquarters level." This rule was qualified by Attorney General Order No. 1623-92 of August 31, 1992, which, in relation to the Federal Bureau of Investigation (FBI), authorized delegation of this approval function to Special Agents in Charge. Experience has shown that the requirement of Special Agent in Charge approval can result in a loss of investigative opportunities because of an overly long approval process, and indicates that allowing approval by Assistant Special Agents in Charge would facilitate FBI investigative operations. Assistant Special Agents in Charge are management personnel to whom a variety of supervisory and oversight responsibilities are routinely given; generally, they are directly involved and familiar with the circumstances relating to the propriety of proposed uses of the consensual monitoring technique. Part V. is accordingly revised in this Memorandum to provide that the FBI Director's designees for purposes of oral authorization of consensual monitoring may include both Special Agents in Charge and Assistant Special Agents in Charge. This supersedes Attorney General Order No. 1623-92, which did not allow delegation of this function below the level of Special Agent in Charge.

Third, this Memorandum omits as obsolete Part VI. of the Memorandum of January 20, 1998. Part VI. imposed a reporting requirement by agencies concerning consensual monitoring but rescinded that reporting requirement after one year.

acting with the consent of a party to a communication, to engage in warrantless monitoring of wire (telephone) communications and oral, nonwire communications. See United States v. White, 401 U.S. 745 (1971); United States v. Caceres, 440 U.S. 741 (1979). Similarly, the Constitution and federal statutes permit federal agents to engage in warrantless monitoring of oral, nonwire communications when the communicating parties have no justifiable expectation of privacy. Because such monitoring techniques are particularly effective and reliable, the Department of Justice encourages their use by federal agents for the purpose of gathering evidence of violations of federal law, protecting informants or undercover law enforcement agents, or fulfilling other, similarly compelling needs. While these techniques are lawful and helpful, their use in investigations is frequently sensitive, so they must remain the subject of careful, self-regulation by the agencies employing them.

The sources of authority for this Memorandum are Executive Order No. 11396 ("Providing for the Coordination by the Attorney General of Federal Law Enforcement and Crime Prevention Programs"); Presidential Memorandum ("Federal Law Enforcement Coordination, Policy and Priorities") of September 11, 1979; Presidential Memorandum (untitled) of June 30, 1965, on, inter alia, the utilization of mechanical or electronic devices to overhear nontelephone conversations; the Paperwork Reduction Act of 1980 and the Paperwork Reduction Reauthorization Act of 1986, as amended; and the inherent authority of the Attorney General as the chief law enforcement officer of the United States.

I. DEFINITIONS

As used in this Memorandum, the term "agency" means all of the Executive Branch departments and agencies, and specifically includes United States Attorneys' Offices which utilize their own investigators, and the Offices of the Inspectors General.

As used in this Memorandum, the terms "interception" and "monitoring" mean the aural acquisition of oral communications by use of an electronic, mechanical, or other device. Cf. 18 U.S.C. § 2510(4).

As used in this Memorandum, the term "public official" means an official of any public entity of government, including special districts, as well as all federal, state, county, and municipal governmental units.

II. NEED FOR WRITTEN AUTHORIZATION

A. Investigations Where Written Department of Justice Approval is Required

A request for authorization to monitor an oral communication without the consent of all parties to the communication must be approved in writing by the Director or Associate Director of the Office of Enforcement Operations, Criminal Division, U.S. Department of Justice, when it is known that:

(1) the monitoring relates to an investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years;

(2) the monitoring relates to an investigation of the Governor, Lieutenant Governor, or Attorney General of any State or Territory, or a judge or justice of the highest court of any State or Territory, and the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his or her official duties;

(3) any party to the communication is a member of the diplomatic corps of a foreign country;

(4) any party to the communication is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers;

(5) the consenting or nonconsenting person is in the custody of the Bureau of Prisons or the United States Marshals Service; or

(6) the Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, or the United States Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent before conducting consensual monitoring in a specific investigation.

In all other cases, approval of consensual monitoring will be in accordance with the procedures set forth in part V. below.