B. Monitoring Not Within Scope of Memorandum

Even if the interception falls within one of the six categories above, the procedures and rules in this Memorandum do not apply to:

(1) extraterritorial interceptions;

(2) foreign intelligence interceptions, including interceptions pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801, et seq.);

(3) interceptions pursuant to the court-authorization procedures of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended (18 U.S.C. § 2510, et seq.);

(4) routine Bureau of Prisons monitoring of oral communications that are not attended by a justifiable expectation of privacy;

(5) interceptions of radio communications; and

(6) interceptions of telephone communications.

III. AUTHORIZATION PROCEDURES AND RULES

A. Required Information

The following information must be set forth in any request to monitor an oral communication pursuant to part II.A.:

(1) **Reasons for the Monitoring.** The request must contain a reasonably detailed statement of the background and need for the monitoring.

(2) **Offense.** If the monitoring is for investigative purposes, the request must include a citation to the principal criminal statute involved.

(3) **Danger.** If the monitoring is intended to provide protection to the consenting party, the request must explain the nature of the danger to the consenting party.

(4) **Location of Devices.** The request must state where the monitoring device will be hidden: on the person, in personal effects, or in a fixed location.
(5) Location of Monitoring. The request must specify the location and primary judicial district where the monitoring will take place. A monitoring authorization is not restricted to the original district. However, if the location of monitoring changes, notice should be promptly given to the approving official. The record maintained on the request should reflect the location change.

(6) Time. The request must state the length of time needed for the monitoring. Initially, an authorization may be granted for up to 90 days from the day the monitoring is scheduled to begin. If there is the need for continued monitoring, extensions for additional periods of up to 90 days may be granted. In special cases (e.g., "fencing" operations run by law enforcement agents or long-term investigations that are closely supervised by the Department's Criminal Division) authorization for up to 180 days may be granted with similar extensions.

(7) Names. The request must give the names of persons, if known, whose communications the department or agency expects to monitor and the relation of such persons to the matter under investigation or to the need for the monitoring.

(8) Attorney Advice. The request must state that the facts of the surveillance have been discussed with the United States Attorney, an Assistant United States Attorney, or the previously designated Department of Justice attorney responsible for a particular investigation, and that such attorney advises that the use of consensual monitoring is appropriate under this Memorandum (including the date of such advice). The attorney must also advise that the use of consensual monitoring under the facts of the investigation does not raise the issue of entrapment. Such statements may be made orally. If the attorneys described above cannot provide the advice for reasons unrelated to the legality or propriety of the consensual monitoring, the advice must be sought and obtained from an attorney of the Criminal Division of the Department of Justice designated by the Assistant Attorney General in charge of that Division. Before providing such advice, a designated Criminal Division Attorney shall notify the appropriate United States Attorney or other attorney who would otherwise be authorized to provide the required advice under this paragraph.

(9) Renewals. A request for renewal authority to monitor oral communications must contain all the information required for an initial request. The renewal request must also refer to all previous authorizations and explain why an additional authorization is needed, as well as provide
an updated statement that the attorney advice required under paragraph (8) has been obtained in connection with the proposed renewal.

B. Oral Requests

Unless a request is of an emergency nature, it must be in written form and contain all of the information set forth above. Emergency requests in cases in which written Department of Justice approval is required may be made by telephone to the Director or an Associate Director of the Criminal Division’s Office of Enforcement Operations, or to the Assistant Attorney General, the Acting Assistant Attorney General, or a Deputy Assistant Attorney General for the Criminal Division, and should later be reduced to writing and submitted to the appropriate headquarters official as soon as practicable after authorization has been obtained. An appropriate headquarters filing system is to be maintained for consensual monitoring requests that have been received and approved in this manner. Oral requests must include all the information required for written requests as set forth above.

C. Authorization

Authority to engage in consensual monitoring in situations set forth in part III.A. of this Memorandum may be given by the Attorney General, the Deputy Attorney General, the Associate Attorney General, the Assistant Attorney General or Acting Assistant Attorney General in charge of the Criminal Division, a Deputy Assistant Attorney General in the Criminal Division, or the Director or an Associate Director of the Criminal Division’s Office of Enforcement Operations. Requests for authorization will normally be submitted by the headquarters of the department or agency requesting the consensual monitoring to the Office of Enforcement Operations for review.

D. Emergency Monitoring

If an emergency situation requires consensual monitoring at a time when one of the individuals identified in part III.B. above cannot be reached, the authorization may be given by the head of the responsible department or agency, or his or her designee. Such department or agency must then notify the Office of Enforcement Operations as soon as practicable after the emergency monitoring is authorized, but not later than three working days after the emergency authorization.

The notification shall explain the emergency and shall contain all other items required for a nonemergency request for authorization set forth in part III.A. above.
IV. SPECIAL LIMITATIONS

When a communicating party consents to the monitoring of his or her oral communications, the monitoring device may be concealed on his or her person, in personal effects, or in a fixed location. Each department and agency engaging in such consensual monitoring must ensure that the consenting party will be present at all times when the device is operating. In addition, each department and agency must ensure: (1) that no agent or person cooperating with the department or agency trespasses while installing a device in a fixed location, unless that agent or person is acting pursuant to a court order that authorizes the entry and/or trespass, and (2) that as long as the device is installed in the fixed location, the premises remain under the control of the government or of the consenting party. See United States v. Yoinn, 702 F.2d 1341, 1347 (11th Cir.), cert. denied, 464 U.S. 917 (1983) (rejecting the First Circuit's holding in United States v. Padilla, 520 F.2d 526 (1st Cir. 1975), and approving use of fixed monitoring devices that are activated only when the consenting party is present). But see United States v. Shabazz, 883 F. Supp. 422 (D. Minn. 1995).

Outside the scope of this Memorandum are interceptions of oral, nonwire communications when no party to the communication has consented. To be lawful, such interceptions generally may take place only when no party to the communication has a justifiable expectation of privacy, or when authorization to intercept such communications has been obtained pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. § 2510, et seq.) or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801 et seq.). Each department or agency must ensure that no communication of any party who has a justifiable expectation of privacy is intercepted unless proper authorization has been obtained.

V. PROCEDURES FOR CONSENSUAL MONITORING WHERE NO WRITTEN APPROVAL IS REQUIRED

Prior to receiving approval for consensual monitoring from the head of the department or agency or his or her designee, a representative of the department or agency must obtain advice that the consensual monitoring is both legal and appropriate from the United States Attorney, an Assistant United States Attorney, or the Department of Justice attorney responsible for a particular investigation. The advice may be obtained orally from the attorney. If the attorneys described above cannot provide this advice for reasons unrelated to the legality or propriety of the consensual monitoring, the advice must be

---

3For example, burglars, while committing a burglary, have no justifiable expectation of privacy. Cf. United States v. Pui Kan Lam, 483 F.2d 1202 (2d. Cir. 1973), cert. denied, 415 U.S. 984 (1974).
sought and obtained from an attorney of the Criminal Division of the Department of Justice designated by the Assistant Attorney General in charge of that Division. Before providing such advice, a designated Criminal Division Attorney shall notify the appropriate United States Attorney or other attorney who would otherwise be authorized to provide the required advice under this paragraph.

Even in cases in which no written authorization is required because they do not involve the sensitive circumstances discussed above, each agency must continue to maintain internal procedures for supervising, monitoring, and approving all consensual monitoring of oral communications. Approval for consensual monitoring must come from the head of the agency or his or her designee. Any designee should be a high-ranking supervisory official at headquarters level, but in the case of the FBI may be a Special Agent in Charge or Assistant Special Agent in Charge.

Similarly, each department or agency shall establish procedures for emergency authorizations in cases involving non-sensitive circumstances similar to those that apply with regard to cases that involve the sensitive circumstances described in part III.D., including obtaining follow-up oral advice of an appropriate attorney as set forth above concerning the legality and propriety of the consensual monitoring.

Records are to be maintained by the involved departments or agencies for each consensual monitoring that they have conducted. These records are to include the information set forth in part III.A. above.

VI. GENERAL LIMITATIONS

This Memorandum relates solely to the subject of consensual monitoring of oral communications except where otherwise indicated. This Memorandum does not alter or supersede any current policies or directives relating to the subject of obtaining necessary approval for engaging in nonconsensual electronic surveillance or any other form of nonconsensual interception.
Digital Dealers

-Sellers of illegal drugs like GHB are finding a brand-new marketplace on the street corners of the information superhighway.

Tuesday 2/26 at 8:30 p.m. Eastern on 'CyberCrime.'
Also airs Saturday 3/2 at 9:30 a.m., 3 p.m., and 7 p.m., Sunday 3/3 at 12 a.m., 11 a.m., 6:30 p.m., and 9:30 p.m., and Tuesday 3/4 at 11 a.m., 1:30 p.m., 6 p.m., and 11:30 p.m.

By Jack Karp
February 26, 2002

Webvan. Kozmo. Peapod. Amazon.com. Fueled by the Internet revolution, companies like these changed the way many of us shop, letting us make purchases from our living rooms and have products delivered to our doors. And though many of these businesses have disappeared as the economy has taken a downturn, one segment of the online delivery industry is booming: drug dealing.

"The majority [of users] seem to be getting it from the Internet," retired narcotics detective Trinka Porrata told "CyberCrime" about gamma hydroxybutyrate (GHB), also known as the date-rape drug.

GHB is one of the most popular drugs available on the Web, according to Porrata, who now works as a drug consultant with Project GHB, a program aimed at raising awareness of GHB addiction and helping GHB addicts recover. GHB, which is colorless, odorless, and almost tasteless, was given its nickname because it is sometimes slipped into an unsuspecting woman's drink, causing several hours of unconsciousness. It disappears from the body within 12 hours and leaves the victim with little or no memory of what happened, making it an ideal drug for would-be rapists.

But GHB is much more popular among recreational users, Porrata said.

"It is far more widespread than anyone wants to believe," she said. "Make no mistake, the use of it for drug-facilitated sexual assault is far greater than really captured by any statistics, but that isn't the bulk of its use... Most of the addicts we deal with are not partygoers, but are gym-goers who were introduced to it as a sleep or workout aid."

In fact, GHB first came to prominence in the 1980s when bodybuilders began using the chemical to stimulate muscle growth and aid sleep. For years, the drug was widely available in health food stores until doctors became aware that it was unsafe.
"GHB is very, very addictive," according to Dr. Alex Stalcup, medical director of the New Leaf Treatment Center in Concord, California. "[Users] progressively lose control over their use. They use it when they shouldn't, they use it in the wrong amounts," Stalcup said. They exhibit "all the signs that they are having trouble controlling use, which is the centerpiece of addiction."

The drug can also be deadly, Stalcup said. "People die because of respiratory depression -- they stop breathing. Some people have died... in the course of GHB-induced convulsions," he said.

And some users fall into depressive states so severe they do not respond to medical treatments. Some become suicidal and kill themselves.

As a result of these dangers, the Food and Drug Administration (FDA) banned the over-the-counter sale of GHB in 1990, making its use illicit except under strict guidelines and when monitored by a doctor. And in February 2000, President Clinton reclassified GHB as a Schedule I drug having no medical use, and possession of GHB became a felony punishable by up to 20 years in prison.

But the change in the law has done little to stem the drug's sale, especially online.

A brief Web search for the term "GHB" yields several websites that offer GHB kits for purchase. The kits usually include GHB precursors like 1,4-butanediol or gamma butyrolactone (GBL), along with sodium hydroxide or potassium hydroxide. And other sites like ghbinfo.org provide recipes for turning the kits' ingredients into GHB.

"The process is quite simple, and does not require complex laboratory equipment," the Drug Enforcement Agency's 2000 Drug Intelligence Brief reported. The report notes that kits sell for anywhere from $48 to $200.

Those kits became extremely popular. In September 1998, shortly before being arrested, Jose Perez-Menchaca bragged to an undercover FDA agent that he had netted approximately $300,000 selling GHB kits over the Internet. In March 1999, Florida authorities arrested three 20-year-old men, two of them students at Florida State University, also for allegedly using the Internet to sell GHB kits. One of the men was captured while attempting to mail 58 boxes containing 211 kits. And earlier this year, two Arkansas brothers plead guilty in a New Jersey court to making approximately $200,000 selling GHB kits online.

"The [kits] are getting a little more difficult to find for a newcomer," Porrata said about these recent enforcement efforts. So, online drug dealers are now getting "sneakier about it." Many of them don't even bother offering the kits any longer, but simply sell GHB analogs -- chemicals like GBL and 1,4-butanediol that are converted by the body into GHB when consumed. The analogs are often legal because they can also be used as industrial cleaners. 
and solvents, and, as a result, many websites sell the chemicals "disguised as a weight belt or ink jet cartridge cleaner," according to Porrata.

"No manufacturing is involved, so it's less serious if you're caught and arrested," Porrata said. "And not all [states] have the analogs covered properly... If I find the website located in a state where it isn't covered, local cops might not be able to do much about it."

GHB isn't the only illicit drug showing up on the street corners of the information superhighway. To find out what else you can score online, take a look at Part 2 of our story.

Drugs: a Business Model

GHB is far from the only illicit drug being sold on the Internet. In March of last year, Keith Hellawell, Britain's anti-drugs minister, reported that there were approximately 1,100 websites around the world selling illegal drugs ranging from marijuana to heroin.

But it's not only the stereotypical street dealers who are looking to muscle in on the new territory the Internet provides. As with any other niche market on the Web, a number of entrepreneurs hope to take advantage of the popularity of drugs with the wired generation.

One of the most publicized and ambitious of these companies is iToke, an Amsterdam-based business that plans to offer customers around the world the chance to purchase marijuana online. Customers who place orders on the iToke website would have their pot delivered via bicycle messenger. And just like with pizza, if the drugs don't arrive within 30 minutes, they're free.

"At the end of the day, who do you want to buy from?" asked Mike Tucker, one of iToke's founders, in an early press release. "Some guy in an alley in Barcelona or from a company that not only delivers premium products but also shows an interest in the community and its employees."

Tucker, who started the company along with fellow American Tim Freccia, is so intent on lending the business of online marijuana sales respectability that the two men reportedly designed the iToke site to look like a cross between the commercial websites for Apple Computer and Starbucks.
"We wanted to set up a business that our contemporaries would respond to -- the Generation X or Slacker generation who all of a sudden have found themselves in the forefront of the new economy," Frecci said in an interview last year with the UK's Independent. "We realized the people we grew up with are probably now Seattle tech workers pulling in a joint salary of around a quarter of a million dollars. They've got houses and kids, but they still smoke pot in the basement."

But the brick-and-mortar marijuana retailers in Amsterdam are not yet willing to accept their new business rival. Originally scheduled to begin delivery service in September 2000, iToke has delayed its launch due to resistance from Amsterdam's coffee shop owners, who currently maintain somewhat of a monopoly on legal marijuana sales in that city. As a result, the iToke website currently sells only T-shirts, polos, and oxfords emblazoned with the iToke logo on the front and the label "User" on the back.

The site has met with considerable success, though, despite the fact that it hasn't yet sold a single ounce of pot. It received approximately 100 million visitors in its first six months and continues to attract around 30,000 visitors each day.

And iToke isn't the first website to try to break into the marketplace. As early as March 1996, another Amsterdam-based website, known as Neuroroom, began selling marijuana, hashish, and ecstasy to customers in 15 countries, including the United States. The drugs would be sent via snail mail to customers who made "donations" to the site. Sellers claimed to have a 90 percent success rate sending small amounts of drugs through the mail until Dutch police shut down the site in 1997.

Another site, Dutchjoints.com, stopped offering marijuana deliveries when it became so popular that its operator, a 41-year-old Dutch limousine driver, began to fear police intervention. He still offers the service, but only to previous customers. And the eBay of e-drugs -- PotPrice.com -- serves as a message board where marijuana sellers can advertise their products and hook up with buyers, even though the site claims to be for entertainment purposes only.

Porrata said drug laws need to be enforced online as well as off.

"The two big needs in this area are training for law enforcement regarding cybercrimes, investigation techniques and training for prosecution," she said. "Many agencies, especially state or local, don't have the manpower to allow time for such cases. The Feds have shown limited interest."

Despite whatever interest law enforcement shows in stopping online drug sales, however limited, police will have to face a growing number of wired dealers who can operate with a certain degree of anonymity and from outside the United States. Porrata said these qualities of the Internet allow dealers to be especially aggressive.

"I was really annoyed when a Chinese chemical supplier of some sort got onto our message board for GHB addicts who are trying to get and stay clean," she said, "advertising to buy GHB from them."

This article was first published on October 9, 2001 and is based on original reporting by "CyberCrime" segment producer Jon Taylor.
Two Men Face Charges For Selling Drug Kits Online

A case involving online kits for manufacturing the date rape drug GHB is arousing a whole new controversy.

August 17, 1999

In a case filed by the Michigan attorney general's office, two men have been criminally charged with solicitation to manufacture a controlled substance—the "date rape drug" known as GHB—over the Internet. They now face up to 30 years in prison.

The men were allegedly running a website that sold do-it-yourself GHB kits for $200 each. GHB can cause intoxication followed by deep sedation, lasting up to eight hours. It gained notoriety as a "date rape" drug after reports in which women were being fed GHB to disinhibit them; in one 1996 case in La Porte, Texas, a 17-year-old girl died after being given a soda spiked with the drug.

According to Michigan Attorney General Jennifer Granholm, this is the first case in which felony criminal charges have been brought against someone for distributing illegal drugs on the Internet. Also, because GHB is legal in many states and is approved by the FDA as a treatment for ailments such as narcolepsy, the case is stirring controversy about whether website operators should have to know the law in every state to which they sell their products.

For CyberCrime Analyst Luke Reiter's full story, click on the video icon above.

Return to Regular View

Copyright © 2001 TechTV LLC. All Rights Reserved.
Use of techtv.com is subject to certain Terms and Conditions. We respect your privacy.

"A people who mean to be their own governors, must arm themselves with the power knowledge gives." – James Madison

NEW 108th Congress Begins With Privacy Briefing
The House Committee on Energy and Commerce held a televised hearing today on the Federal Trade Commission's proposal for a national "Do Not Call" list. The proposal is strongly favored by the FTC and consumer organizations. See EPIC's Telemarketing page. (Jan. 8)

NEW INS Seeks Info on Citizens Who Travel
The Immigration and Naturalization Service (INS) has proposed a new rule that would require all individuals leaving or entering the United States -- including U.S. citizens -- to provide certain personal information to the government. The required data would include complete name, date of birth, address and passport number. Such identification requirements currently apply only to non-resident aliens. Public comments on the proposed rule may be submitted until February 3. (Jan. 7)

Court Rules for EPIC in Homeland Security FOIA Case
U.S. District Judge Colleen Kollar-Kotelly has issued a decision (PDF) permitting EPIC to pursue discovery concerning the "nature of the authority" delegated to the Office of Homeland Security (OHS) and its Director, Tom Ridge. The ruling comes in response to a Freedom of Information Act lawsuit filed by EPIC after OHS took the position that it is not subject to the open government law. (Jan. 2, 2003)

EPIC Files Comments on Canadian Surveillance Proposal
EPIC has submitted recommendations (PDF) on a government proposal (PDF) that would require telecommunications and Internet service providers to enable broader police surveillance of private communications. The comments expressed support for the views of Canadian civil liberties organizations. (Dec. 19, 2002)

Pentagon Makes Incomplete Response to TIA FOIA Request
After EPIC filed suit (PDF) challenging its failure to release documents about the controversial "Total Information Awareness" program, the Defense Department has provided one document -- a study titled "Security with Privacy" (PDF, 840K). The study recommends more DoD research on privacy, but does not address policy issues and states that it is "not a review of Total Information Awareness." (Dec. 19)

FTC Announces National Do-Not-Call List
The FTC will establish a national DNC list that will accommodate both Internet and toll-free phone number enrollment. The new regulations also require telemarketers to transmit caller ID information, establish new rules for the use of preacquired account number information, and prohibit "abandoned" calls. For the list to operate, Congress will have to approve the levying of charges to the telemarketing industry in order to fund the program. EPIC and a coalition of consumer and civil liberties groups submitted detailed comments in favor of a DNC list. For more information, see the EPIC Telemarketing Page. (Dec. 18)
EPIC Asks Appeals Court to Reconsider Faxed Warrant
EPIC filed a response (PDF) to a petition for reconsideration in the Eighth Circuit, urging the Circuit to reconsider a November ruling (PDF) that service of a warrant on an ISP by fax complies with the "reasonableness" requirements of the Fourth Amendment. EPIC filed an amicus brief (PDF) in the case, arguing that U.S. search and seizure law has mandated officer presence at the service of a warrant since the 1700s. EPIC's latest filing argues that the November opinion didn't adequately consider the distinction between service of a warrant and execution of a warrant. For more information, see EPIC's Back Page. (Dec. 17)

Previous EPIC Top News

EPIC Resources and Guides

EPIC Alert
The current and back issues of EPIC's award-winning newsletter on civil liberties in the information age. Subscribe now

EPIC's Bill-Track
Track pending legislation on Privacy and Cyber-Liberties in the 107th Congress.

EPIC Bookstore
Browse the cyber shelves of good books on privacy, free speech, and civil liberties at the Internet's only bookstore devoted to online freedom. Shipping, discounts, and gift wrapping provided!

EPIC Events
A listing of important upcoming and past events dealing with privacy and First Amendment issues.

Former Secrets
View scanned images of previously classified government documents obtained by EPIC under the Freedom of Information Act.

EPIC's Online Guide to Practical Privacy Tools
Information on how to get PGP, RSA SecurPC, and other encryption programs, anonymous remailers and surfing the net anonymously.

EPIC's Online Guide to Privacy Resources
All the best sites, newsletters, conferences, and organizations on and off the net.

EPIC Reports
Read reports available online, including the new "Watching the Watchers" series, or click through to the EPIC Bookstore and purchase hard copies of publications.

EPIC Policy Archives

Computer Security
Is Cyberspace secure? Hackers, information warfare, laws and guidelines. Includes resources on Critical Infrastructure Protection.

Cryptography Policy
Who holds the keys to online privacy? Clipper-Chip, key escrow, expert controls.
reports and more.

**Free Speech**
Freedom of speech issues on the Internet including anonymous speech, liability, censorship, and the pending challenge to the Child Online Protection Act. EPIC's Faulty Filters report is also online.

**Freedom of Information**
How to use the Freedom of Information Act (FOIA) and other laws to obtain information on government activities. See documents EPIC has obtained. Learn how to get your own files.

**Privacy**
The A to Z's of privacy. From airline passenger profiling and Caller ID to Social Security Numbers and Wiretapping.

**About EPIC**
EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.

**EPIC's Litigation Docket**
Learn about the privacy, First Amendment, and Freedom of Information Act court cases brought by the legal team at EPIC. Defending your rights in cyberspace!

**EPIC Advisory Board and Staff**
The people behind EPIC and their pages.

**Contribute to EPIC**
We have no clients, no customers, and no shareholders. We need your support. Here’s how to help out. You can also make contributions to EPIC by credit card.

**Praise for EPIC and the EPIC site cited (and sighted)**
Kind words and places to find EPIC.ORG.

**EPIC Privacy Policy**
What we don’t do with your personal information.

Electronic Privacy Information Center  
1718 Connecticut Avenue, NW, Suite 200  
Washington, DC 20009  

+1 202 483 1140 (tel) +1 202 483 1248 (fax)  
http://www.epic.org/ - info@epic.org

file://A:\Electronic%20Privacy%20Information%20Center.htm  
1/9/2003
Wiretapping

News | Digital Telephony | Other Resources

The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping.


News

- **U.S. Customs Surveillance Records Lost in 9-11 Attacks.** The number of federal and state police authorized wiretaps increased again this year, mostly due to drug investigations. Wired.com reports that the actual number of authorized wiretaps is likely to be higher than reported, since U.S. Customs surveillance records were lost in the destruction of the World Trade Center. It is not clear whether the results of the wiretaps were lost, or whether merely the records from which the reporting would be done—which would skew the results of the annual wiretap reports.

- **FCC Again Approves FBI’s CALEA Requirements.** The Federal Communications Commission issued an "Order on Remand" (PDF) on April 11 reinstating the mandated surveillance capabilities that were rejected by the D.C. Circuit Court of Appeals in 2000. (April 16)

- **DOJ Issues Guidance on New Surveillance Powers.** Within hours of the USA PATRIOT Act being signed into law, the Justice Department issued a field guidance memorandum (PDF) on the new anti-terrorism authorities approved by Congress. The memorandum does not address expanded powers under the Foreign Intelligence Surveillance Act; guidance in that area appears to be classified. Attorney General John Ashcroft announced that he has directed FBI and U.S. Attorney's offices "to begin immediately implementing this sweeping legislation." (Oct. 29, 2001)

- **Anti-Terrorism Bill Signed Into Law.** On October 26, the President signed the USA-PATRIOT Act of 2001 into law. The Senate voted 98-1 to pass the Act, a "compromise" version of the various anti-terrorism bills, on October 25. This final congressional action followed 24 hours after the House voted 357-66 to approve the same version of the bill, based on H.R. 3108 and S. 1510. The final legislation includes a few changes: most notably, a sunset on the electronic surveillance provisions, and an amendment providing judicial oversight of law enforcement's use of the FBI's Carnivore system. However, it retains provisions vastly expanding government investigative authority, especially with respect to the Internet. (Oct. 26, 2001)

- **Congress Set to Consider Far-Reaching Terrorism Proposal.** Congressional committees will hold hearings on Monday and Tuesday to consider broad legislation proposed by the Department of Justice that would, among other things, substantially expand government surveillance powers, including use of the controversial Carnivore Internet monitoring system. EPIC has prepared a
detailed analysis of provisions in the proposed Anti-Terrorism Act of 2001 (PDF) that would affect communications and information privacy. EPIC urges Congress to carefully assess the need for new surveillance powers and to draw any possible changes narrowly to protect privacy and constitutional rights. In editorials, newspapers and magazines across the country have also endorsed that approach. (Sept. 24, 2001)

- Appeals Court Limits Use of New Surveillance Techniques. The U.S. Court of Appeals for the D.C. Circuit has ruled that law enforcement agencies must meet the highest legal standard before using new surveillance capabilities. The court decision came in a legal challenge filed by EPIC, other privacy groups and the telecommunications industry to invalidate technical surveillance standards issued by the Federal Communications Commission last year. The capabilities, which include cellular phone location tracking and surveillance of "packet mode" data, were ordered implemented by the FCC under the Communications Assistance to Law Enforcement Act (CALEA). Several other technical capabilities were completely rejected by the court.

- FBI System Takes a Bite Out of Privacy. The Federal Bureau of Investigation has a rolled out a new system to monitor private communications — "Carnivore." The first public discussion of the system was contained in Congressional testimony delivered earlier this year. EPIC has filed a Freedom of Information Act request for details. See EPIC's Carnivore Page for declassified FBI documents and other information.


- Court of Appeals Hears CALEA Case. The U.S. Court of Appeals for the DC Circuit had oral arguments on CALEA on May 18. The court heard from lawyers representing USTA, EPIC, FCC and the FBI. The court is expected to issue its ruling later this year.

- Privacy Groups Challenge FBI Wiretap Standards. EPIC, ACLU and EFF have asked a federal appeals court to block new rules that would permit the FBI to dictate the design of the nation's communication infrastructure. The challenged rules would enable the Bureau to track the physical locations of cellular phone users and potentially monitor Internet traffic. The appellate brief (PDF version available) challenges an FCC order implementing the Communications Assistance to Law Enforcement Act (CALEA). See the joint press release for additional information.

The Digital Telephony Law (CALEA)

On the last night of the 1994 session, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA), sometimes called the "Digital Telephony" bill. CALEA requires telephone firms to make it easy to wiretap the nation's communication system. The bill faced strong opposition from industry and civil liberties organizations, but was adopted in the closing hours of Congress after the government offered to pay telephone companies $500,000,000 to make the proposed changes. EPIC opposed passage of the bill and believes that the government has failed to justify the $500,000,000 appropriation required.

As part of the final omnibus funding bill enacted in the last days of the 104th Congress, the
Congress approved a provision allowing for funding the digital telephony bill from money reprogrammed from intelligence and law enforcement agencies.

- The text of the Communications Assistance for Law Enforcement Act of 1994
- Legislative history of the Communications Assistance for Law Enforcement Act (House Report No. 103-827)

Recent Developments

- **NEW** FCC Again Approves FBI's CALEA Requirements. The Federal Communications Commission issued an "Order on Remand" (PDF) on April 11 reinstituting the mandated surveillance capabilities that were rejected by the D.C. Circuit Court of Appeals in 2000. (April 16)

- Appeals Court Limits Use of New Surveillance Techniques. The U.S. Court of Appeals for the D.C. Circuit has ruled that law enforcement agencies must meet the highest legal standard before using new surveillance capabilities. The court decision came in a legal challenge filed by EPIC, other privacy groups and the telecommunications industry to invalidate technical surveillance standards issued by the Federal Communications Commission last year. The capabilities, which include cellular phone location tracking and surveillance of "packet mode" data, were ordered implemented by the FCC under the Communications Assistance to Law Enforcement Act (CALEA). Several other technical capabilities were completely rejected by the court.

- Court of Appeals Hears CALEA Case. The US Court of Appeals for the DC Circuit had oral arguments on CALEA on May 18. The court heard from lawyers representing USTA, EPIC, FCC and the FBI. The court is expected to issue its ruling this summer.

- Privacy Groups Challenge FBI Wiretap Standards. EPIC, ACLU and EFF have asked a federal appeals court to block new rules that would permit the FBI to dictate the design of the nation's communication infrastructure. The challenged rules would enable the Bureau to track the physical locations of cellular phone users and potentially monitor Internet traffic. The appellate brief (PDF version available) challenges an FCC order implementing the Communications Assistance to Law Enforcement Act (CALEA). See the joint press release for additional information.

- FCC Okays FBI Cell Phone "Location Tracking" Request. In a statement released on October 22, 1999, the Federal Communications Commission expressed its initial approval of FBI-proposed technical requirements that would enable law enforcement to determine the location of individuals using cellular telephones. A formal Notice was released on November 5. The Commission rejected other capabilities requested by the Bureau and deferred decisions on other issues, including surveillance of Internet communications. The initial decision came in a proceeding under the controversial Communications Assistance to Law Enforcement Act (CALEA).

- FCC Approves FBI Wiretap Standards for Telecom Networks. EPIC has expressed its concern that a Federal Communications Commission (FCC) decision issued on August 27 could result in a significant increase in government interception
of digital communications (see **FCC press release** for summary). In its decision, the FCC largely has adopted technical standards proposed by the Federal Bureau of Investigation (FBI) that would dictate the design of the nation's telecommunications networks. Included is a requirement that cellular telephone networks must have the ability to track the physical location of cell phone users.

- **EPIC Urges FCC to Protect User Privacy.** EPIC, joined by the American Civil Liberties Union and the Electronic Frontier Foundation, has filed formal comments with the Federal Communications Commission urging it to reject FBI-proposed technical requirements that would -- among other things -- enable law enforcement to determine the location of individuals using cellular telephones. Also at issue is surveillance of Internet communications. The comments on implementation of the controversial Communications Assistance to Law Enforcement Act (CALEA) were filed on December 14. In a statement released on October 22, the Commission expressed its initial approval of the FBI proposal. A formal Notice was released on November 5.

- **Phone Companies Sue FBI Over Wiretapping Law.** The U.S. Telephone Association, which represents over 1,200 local phone companies (including the Baby Bells), filed suit on August 19 against the FBI and DOJ over implementation of the Communications Assistance for Law Enforcement Act (CALEA).

- **Groups Ask FCC to Delay Wiretap Law.** Industry and public groups filed petitions on May 8 asking the FCC to delay the implementation of CALEA. Comments filed by EPIC, ACLU & EFF asking for indefinite delay until controversy over standards is resolved.

- **Wireless Phone Companies Sue FBI for Wiretap Costs.** The Cellular Telephone Industry Association and the Personal Communications Industry Association filed a lawsuit on April 27 against the DOJ and FBI. The companies say that the FBI's new regulations on CALEA unlawfully shifts the cost of paying for phone equipment upgrades for wiretapping from the FBI to the telephone companies.

- **FBI Issues Final Capacity Requirements.** The Federal Bureau of Investigation sets out wiretap requirements for the nation's telephone system. Companies are expected to comply by October 1998. EPIC and other cyber-liberties groups have sent a letter to Congress and filed comments with the FCC asking for a review of the Bureau's actions. The groups say the FBI has acted in "bad faith" in seeking to implement a massive wiretapping scheme. Rep. Bob Barr (R-GA) has introduced the CALEA Implementation Amendments of 1998 which would delay implementation until 2000.

- **EPIC Urges Rejection of FBI Wiretap Initiative.** In formal comments filed with the Federal Communications Commission on May 20, EPIC says the FBI's implementation of the Communications Assistance to Law Enforcement Act (CALEA) -- calling for the redesign of the nation's communications network to facilitate surveillance -- threatens fundamental privacy and constitutional rights.

- **Major Cyber-liberty Groups Call for FCC to Stop Wiretap Law Implementation.** EPIC and other major cyber-liberties groups filed comments with the FCC on February 12 asking the FCC to stop implementation of the Communications Assistance for Law Enforcement Act.
• EPIC, ACLU File Comments on CALEA. ACLU, EPIC and EFF filed comments with the Federal Communications Commission on December 12 calling for delaying the implementation of CALEA until October 2000.

• New Report Reveals EU/FBI Global Surveillance Plans. A newly issued report by Statewatch reveals that the European Union and US FBI have been actively promoting agreements to ensure surveillance of all telecommunications networks. See the Privacy International Phone Tapping page for more information.

Funding Digital Telephony

• Text of the 1996 House bill funding the Digital Telephony bill.

• EPIC's Oppose Digital Telephony Funding Campaign, 1994.

• EPIC's Press Release on campaign to oppose funding of the CALEA.

• Comprehensive file of material opposing wiretap funding, including budget documents, testimony of FBI Director Freeh, and a sample letter.

Early Implementation of CALEA

• The FBI's proposed rule on procedures for recovery of CALEA-related costs by telecommunications carriers (May 10, 1996) (PDF format).

• The FBI's belated report to Congress on annual wiretap expenditures under CALEA.

• The FBI's report on the methodology used to produce its estimate of required wiretap capacity


• EPIC's December 12, 1995, letter to Congress concerning the FBI's failure to produce a statutorily-mandated report on wiretap expenditures.

• Federal Register Notice reveals that the FBI expects to simultaneously monitor one percent of all communications in some regions of the country (October 16, 1995) (PDF format)

• EPIC's formal comments on the FBI's wiretapping capacity requirements (described above).

• FBI Director Freeh's letter to Rep. Henry Hyde on the FBI's wiretapping capacity requirements.

• February 23, 1995 Federal Register Notice concerning implementation of the CALEA.

• FBI Director Freeh's testimony (3/30/95) on the CALEA and cryptography.
Materials on the Enactment of CALEA

- Office of Technology Assessment report "Electronic Surveillance in a Digital Age"

- White House document obtained under FOIA shows Approval of President George Bush and the link between digital telephony and the Clipper Chip. (gif file)


- EPIC's FOIA Wiretap Survey Case against the FBI for the surveys allegedly showing the need for the FBI Digital Telephony Proposal.

- 1992 memos from the General Services Administration (GSA) showing that they opposed the Digital Telephony proposal because it could "adversely affect national security."

Other Wiretap Resources

- Administrative Office of the US Courts Wiretap Reports
  - 2000 Report
  - 1999 Report
  - 1998 Report
  - 1997 Report

- EPIC's Charts and graphics of Title III federal and state wiretaps and bugs 1968 - 1999.


- EPIC's page on Counter-terrorism, including text of Comprehensive Counterterrorism Prevention Act of 1995 and current wiretap expansion proposals.
Identity Theft Resources

- Identity Theft Publications
- Other Identity Theft Sites
- Victims' Stories and Hotline Cases
- Identity Theft Resource Center

Media Alert of Potential Identity Theft Scam Related to Terrori Attacks

Identity Theft Publications

- Fact Sheet 17: Coping with Identity Theft: What to Do When An Im Strikes
- Fact Sheet 17(a): Identity Theft: What to Do When it Happens to Y Guide for Victims
  in Spanish: Robo de identidad: Qué hacer si le sucede a usted
- Fact Sheet 17(b): Organizing Your Identity Theft Case
- Fact Sheet 17(c): Reasonable Requests an Identity Theft Victim M Make of the Courts
- Fact Sheet 17(d): Forming an Identity Theft Victim Support Group
- Fact Sheet 17(e): Identity Theft - Overcoming the Emotional Impac
- Fact Sheet 17(f): The Court Experience: A Guide for Identity Theft Victims
- Fact Sheet 17(g): Criminal Identity Theft
- Fact Sheet 17(j): Enhancing ID Theft Victim - Investigator Commu
- Fact Sheet 17(k): Enhancing Law Enforcement - Identity Theft Communication
• Fact Sheet 17(L): Should I Change My Social Security Number?
• Fact Sheet 17(P): When You Personally Know the Identity Thief
• Victims Stories
• California DMV Identity Theft Hearing Testimony
• Preventing Identity Theft: Industry Practices Are the Key - National Summit on Identity Theft
• Identity Theft: How It Happens, Its Impact on Victims, & Legislative Solutions (U.S. Senate Testimony)
• Identity Theft: The Growing Problem of Wrongful Criminal Records
• "Nowhere to Turn: Victims Speak Out on Identity Theft," report by CALPIRG & PRC
• Identity Theft IQ Test
• Workplace Identity Theft IQ Test

Other Identity Theft Sites

• Identity Theft Resource Center - http://www.idtheftcenter.org/
• U.S.PIRG and CALPIRG - http://www.pirg.org/
• Mari Frank's Identity Theft Survival Kit - http://www.identitytheft.org/id_theft_kit.htm
• Federal Bureau of Investigation - http://www.fbi.gov/contact/fo/norfolk/1999/ident.htm
• FBI Internet Fraud Complaint Center - http://www.ifccfbi.gov/
• Web Site of Bay Area ID Theft Activist - http://boojiboy.eorbit.net/~tracey/idtheft/
VICTIMS' STORIES AND HOTLINE CASES:

- Victims' Stories
- Cases 1996-1997
- Cases 1995-1996
- Cases 1994-1995

IDENTITY THEFT RESOURCE CENTER

The ITRC is an affiliated program of the Privacy Rights Clearinghouse. Its website, http://www.idtheftcenter.org/, offers numerous resources for victims of identity theft as well as those who are working to prevent the crime.

©Copyright 1998 - 2002
Last Modified: October 21, 2002

PRIVACY RIGHTS CLEARINGHOUSE

Fact Sheets | Páginas Informativas | New Postings & Alerts | Speeches & Testimony | About Us
Identity Theft | Financial Privacy | Internet Privacy | Privacy Links | Sample Letters
Support Us | Consumers Speak Out | Join our Mailing List | Contact Us | Privacy Policy | Search Our Site | Home
In August 1988, relying on a confidential informant's tip, officers of the Torrance Police Department...
began surveillance of a house at 23302 Anza in Torrance, California. Police continued this surveillance from September 1 through September 6, 1988.

On September 3, 1988, officers followed Julio Balmaceda as he drove from the Anza address to various Western Union offices. The officers observed Balmaceda driving in a "counter-surveillance" manner—he would quickly pull over to the curb and allow cars to pass, he made U-turns, and he circled the neighborhood.

On September 6, 1988, officers observed Manuel Suastegui meet with Balmaceda inside the Anza residence. Officers followed Suastegui as he drove away from the house in a red Ford Bronco. Approximately five miles away, officers observed Anthony Ruiz Del Vizo driving a Plymouth Voyager van. Del Vizo and Suastegui began driving in tandem. Officers observed both using cellular telephones and frequently-checking their rear view mirrors.

Del Vizo stopped for gas at a station in Cerritos. Suastegui parked the Bronco in front of the gas station, approached Del Vizo, and conversed with him. After a few minutes, both men returned to their respective vehicles and continued to drive in tandem.

Del Vizo drove the van to a house located at 13357 Ashworth in Cerritos, where he parked in the driveway and spoke with Manuel Ibarra. Meanwhile, Suastegui drove his Bronco past the Ashworth residence without stopping. Suastegui then made a U-turn and headed back to the gas station where he and Del Vizo had met earlier. When Del Vizo finished his discussion with Ibarra, he returned to the gas station on foot, leaving the van in the driveway of the Ashworth residence. At the gas station, Del Vizo entered Suastegui's Bronco and the two drove to a shopping mall, where they parked and then meandered through the mall.

The surveillance officers remaining at the Ashworth residence noticed that Ibarra came outside to look into Del Vizo's van at least twice in the first five to ten minutes after Del Vizo had left. Approximately thirty minutes later an unidentified male arrived at the Ashworth house in a pick-up truck and met with Ibarra in front of the house. After a brief discussion, the two entered the house. Moments later, the newcomer came out carrying a plastic bag containing a sharp rectangular object inside; the package was of a size that it might have contained a kilogram of cocaine. The unidentified man placed the bag inside a utility box in the rear of his pick-up truck and drove away. The officers observed him circle the area in what appeared to be a counter-surveillance manner before driving onto the freeway.

Ten minutes later, Ibarra left the Ashworth house carrying a box measuring three feet by two feet. Ibarra placed the box inside Del Vizo's van. A few minutes later, Hector Ramos arrived in a pick-up truck and parked. After a brief discussion with Ibarra, Ramos left in Del Vizo's van.

Officers followed the van from the Ashworth house to a house at 12234 Brittain in Hawaiian Gardens. Ramos drove in a counter-surveillance manner from the Ashworth house to the Brittain house: he circled the area, made U-turns, drove faster than the speed limit, and frequently pulled the van to the right curb to let traffic go by before resuming driving. At the Brittain house, Ramos parked the van partially down the driveway. Ramos got out and removed the box that Ibarra had placed in the van; he took the box into the Brittain house.

Twenty minutes later, Ramos exited the house with another individual. Both got into Del Vizio's van and drove to an apartment at 21925 Clareta in Hawaiian Gardens. Again, officers following Ramos saw him drive in a counter-surveillance manner. At the Clareta address (an apartment complex), officers could not see exactly where Ramos went. However, some twenty minutes later, officers saw
Ramos leave, still driving Del Vizo's van. The van now appeared to be carrying some cargo, as it sat lower in the rear. Ramos drove back to the aforementioned Ashworth house in Cerritos. This time, he carefully obeyed all traffic laws, drove well below the posted speed limit, and did not commit any traffic infractions as before.

Back at the Ashworth house, Ramos met briefly with Ibarra after he parked Del Vizo's van in front of the house. Ramos then departed in his pick-up truck. Ibarra went to the rear portion of the van and checked it before going back into the house. Later, Ibarra came out again and checked the doors of the van, apparently to see whether they were locked.

Minutes later, Ibarra exited the house with another individual and drove to a nearby supermarket, where he made telephone calls from a public telephone before returning to the Ashworth house. Minutes later, Del Vizo and Suastegui returned in the Bronco to the Ashworth house. Suastegui there dropped off Del Vizo and then drove off to the nearby gas station; Suastegui appeared to hide at the station. Del Vizo meanwhile met briefly with Ibarra in front of the Ashworth house before getting into the van and driving away.

Del Vizo drove the van more slowly than the existing flow of traffic and allowed other cars to pass him before he got onto the freeway. Minutes later, Suastegui caught up to him on the freeway, and Suastegui's Bronco and Del Vizo's van once again were driven in tandem.

Police officers then decided to make a stop of both vehicles, based upon their observations and their belief that a drug transaction had just occurred. Two marked Torrance patrol cars stopped both the Bronco and van. At a roadblock, Del Vizo was ordered out of the van and forced to lie down on the street; he was then handcuffed. After being handcuffed, Del Vizo was asked whether he spoke English; and he responded affirmatively. He was told that he was being detained pending a narcotics investigation. The officers also asked Del Vizo if he would consent to a search of the Voyager van. Del Vizo consented. When the officers told Del Vizo that he did not have to consent, Del Vizo reaffirmed his consent.

Before searching the van, the police looked into it through its windows. In the back of the van, in plain view through the windows, they could see plastic bags with packages inside. The officers suspected that the bags contained cocaine or other drugs and brought a narcotics-detection dog to the scene. The dog alerted the officers to the presence of drugs in the van. The officers then searched the van and found 104 kilograms of suspected cocaine in the bags. A field test indicated that the substance in the bags was indeed cocaine. The officers also found in the van documents indicating that the van was registered to Del Vizo and specifying Del Vizo's residence. Suastegui and Del Vizo were arrested for narcotics trafficking and their vehicles were impounded.

On September 20, 1988, Del Vizo and six other defendants were indicted on seven counts of various narcotics offenses. Del Vizo pleaded not guilty at his arraignment. Del Vizo also filed a motion to suppress evidence, contending that he had been arrested without probable cause. After an evidentiary hearing, the district court denied the suppression motion on November 7, 1988.

On January 3, 1989, Del Vizo withdrew his pleas of not guilty to two counts of the indictment and entered conditional guilty pleas on those counts. Defendant was sentenced to 190 months' imprisonment and five years' supervised release. The remaining counts were dismissed at the government's motion, and a judgment of conviction was entered on June 17, 1989.

Del Vizo timely appeals the denial of the suppression motion. We have jurisdiction under 28 U.S.C. 1291.
We first inquire whether Del Vizo was under arrest by the time cocaine was discovered in his van. The district court concluded alternatively (1) that Del Vizo's initial detention amounted to a mere investigatory stop which ripened into an arrest only after the discovery of the cocaine, or (2) that there was probable cause to arrest Del Vizo at the time the van was stopped. We conclude that Del Vizo had been arrested prior to the discovery of the cocaine, and treat the question of probable cause in the succeeding section.

In determining whether an official detention has ripened into an arrest, we consider the "totality of the circumstances." United States v. Baron, 860 F.2d 911, 914 (9th Cir. 1988), cert. denied, 490 U.S. 1040, 109 S.Ct. 1944 (1989). There has been an arrest if, under the circumstances, a reasonable person would conclude that he was not free to leave after brief questioning. United States v. Pinion, 800 F.2d 976, 978 -79 (9th Cir. 1986), cert. denied, 480 U.S. 936, 107 S.Ct. 1580, 94 L.Ed.2d 770 (1987); see also United States v. Delgadillo-Velasquez, 856 F.2d 1292, 1295 (9th Cir. 1988) ("we review the situation from the perspective of the person seized").

In this case, the circumstances surrounding Del Vizo's detention included an order to alight from his vehicle and subsequent handcuffing, all done by officers brandishing weapons. Under the totality-of-the-circumstances standard, none of these factors alone is dispositive. For example, holding a suspect at gunpoint does not necessarily convert an investigatory stop into an arrest. See, e.g., United States v. Alvarez, 899 F.2d 833, 838 -39 (9th Cir. 1990) (officers did not arrest defendant when they approached his vehicle with guns drawn and ordered defendant to stop out of his car), petition for cert. filed, 59 U.S.L.W 3180 (U.S. Sept. 5, 1990) (No. 90 -420); United States v. Taylor, 716 F.2d 701, 708 -09 (9th Cir. 1983) (investigatory stop and not arrest occurred when police approached suspects with drawn guns after having been warned that the suspects were dangerous). Similarly, the fact that the officers handcuffed a suspect does not, in itself, automatically escalate a stop into an arrest. See, e.g., United States v. Bautista, 684 F.2d 1286, 1289 -90 (9th Cir. 1982) (handcuffing justified by possibility that another suspect lurked in the vicinity), cert. denied, 459 U.S. 1211, 103 S.Ct. 1206, 75 L.Ed.2d 447 (1983).

In Delgadillo-Velasquez, we were confronted with a situation similar to the one presented in this case. The police in Delgadillo-Velasquez had detained three suspects by approaching the suspects with weapons drawn, ordering them to halt, and requiring them to lie face down in the street while they were handcuffed. We held that at this point the suspects were under arrest. See 856 F.2d at 1295. We observed that "[t]he show of force and detention techniques used in this context are indistinguishable from police conduct in an arrest. . . Clearly, a reasonable innocent person in these circumstances would not have felt free to leave after brief questioning." Id. at 1295-96 (citations omitted).

Although in the instant case the police did not announce to the suspect that he was under arrest, as they did in Delgadillo-Velasquez, the distinction is not pivotal. Even without a statement that he was under arrest, the absolute curtailment of Del Vizo's liberty clearly would have lead a reasonable person to believe that he was not free to leave. Cf. United States v. Strickler, 490 F.2d 378, 380 (9th Cir. 1974) ("No significant, new restraint was added when [an officer] . . . handcuffed Strickler and formally pronounced him 'under arrest'.")

It is true, as the government argues, that an investigatory stop will not be converted into an arrest simply when the officers take "reasonable measures to neutralize the risk of physical harm and to determine whether the person in question is armed." Alvarez, 899 F.2d at 838. However, the officers'
suspicion that Del Vizo may have been involved in drug trafficking did not justify the extent of restraints imposed upon the suspect. There was no evidence that Del Vizo failed to comply with police orders; on the contrary, undisputed testimony in the district court indicated that Del Vizo did exactly as ordered. Cf. Taylor, 716 F.2d at 709 (handcuffing justified where suspect disobeyed orders to raise hands and made furtive movements inside truck). There was no other evidence suggesting that Del Vizo was particularly dangerous, especially once he had stepped out of the van, had been frisked and was lying on the ground. Compare Álvarez, 899 F.2d at 838 -39 (drawn guns did not indicate arrest where police had reason to believe suspect was armed with explosives) and United States v. Greene, 783 F.2d 1364; 1367 -68 (9th Cir.) (no arrest where police were tipped that defendants were armed and police frisked them), cert. denied, 476 U.S. 1185, 106 S.Ct. 2923, 91 L.Ed.2d 551 (1986) with United States v. Roberts, 833 F.2d 777, 781 -82 (9th Cir. 1987) (surrounding suspect and pointing weapons at her amounted to an arrest where officers had no indication that suspect was armed). Indeed, the government cites no case in which we have found "reasonable measures" in a Terry-stop to include drawing weapons on a cooperative suspect, ordering him out of his vehicle and to lie prone on the street, and handcuffing him.

Given the extensive limits placed on Del Vizo's freedom and the lack of an investigatory justification for the degree of these restraints, we have little difficulty concluding that Del Vizo was arrested before the discovery of cocaine in the back of the van.

III

Having determined that Del Vizo was arrested before the discovery of cocaine in his van, we next consider whether there was probable cause to support that arrest. The district court found that the investigating officers possessed probable cause to arrest Del Vizo when they stopped Del Vizo's van. We agree.

An arrest must be supported by probable cause. See Whiteley v. Warden, 401 U.S. 560, 564 -66, 91 S.Ct. 1031, 1034 -36, 28 L.Ed.2d 306 (1971) (same probable-cause standard applies for arrest warrant or warrantless arrest). Probable cause exists when the police know "reasonably trustworthy information sufficient to warrant a prudent person in believing that the accused had committed or was committing an offense." Delgadillo-Velasquez, 856 F.2d at 1296; see also Beck v. Ohio, 379 U.S. 89, 91, 85 S.Ct. 223; 225, 13 L.Ed.2d 142 (1964) (same). Courts look to the totality of the circumstances known to the officers prior to any search conducted incident to the arrest. United States v. Potter, 895 F.2d 1231, 1233-34 (9th Cir.), cert. denied, ___ U.S. ___, 110 S.Ct. 3247, 111 L.Ed.2d 757 (1990). When there has been communication among agents, probable cause can rest upon the investigating agents "collective knowledge." United States v. Bernard, 623 F.2d 551, 560 -61 (9th Cir. 1979).

At the time that Del Vizo was arrested, the police had received a tip that persons residing at 23302 Anza were part of a narcotics organization. They had observed Del Vizo drive his van from Torrance to Cerritos in tandem with co-defendant Suastegui, someone who had been at the Anza residence; during the drive, the two conversed by cellular telephone and frequently appeared to check whether they were being followed. Officers had observed Del Vizo drop off his van at a residence on Ashworth, talk with Ibarra, and then meet Suastegui at a nearby gas station, after which the two drove off together.

At the Ashworth residence, the investigating officers had witnessed Ibarra give a small package to another individual and place a larger package in the van. The officers had observed co-defendant Ramos drive Del Vizo's van (with the package inside) to another address, all the while travelling in a counter-surveillance fashion. Police had witnessed the drop-off of the package from Del Vizo's van and further counter-surveillance driving by Ramos. The officers had observed Ramos visit still another
residence, after which he drove the van, which now appeared to be loaded down, in an especially cautious manner back to the Ashworth residence.

Back at the Ashworth residence, officers had observed Ramos's departure in another vehicle and Ibarra's periodic checks on the parked van. The agents witnessed Ibarra leave his residence to use a pay telephone, after which Del Vizo and Suastegui immediately returned to the Ashworth residence. The officers observed Suastegui dropping off Del Vizo and then hiding out in a gas station. The investigators witnessed Del Vizo meet with Ibarra and then drive off in the van, proceeding cautiously. Finally, the officers observed Suastegui rejoin Del Vizo as the two drove in tandem back toward Torrance.

Many of the observations or circumstances described above have been thought to be indicants of illegal activity. For example, tandem or erratic driving may be indicative of criminal goings-on. See, e.g., United States v. Robert L., 874 F.2d 701, 703 -04 (9th Cir. 1989) (considering evidence of erratic driving and driving in tandem); United States v. Medina-Gasca, 739 F.2d 1451, 1454 (9th Cir. 1984) (considering driving in tandem). Similarly, driving or acting in a counter-surveillance fashion can be another indicant of criminal activity. See, e.g., United States v. Rodriguez, 869 F.2d 479, 483 (9th Cir. 1989) (counter-surveillance driving and parking included in affidavit establishing probable cause); United States v. Hoyos, 892 F.2d 1387, 1393 (9th Cir. 1989) (noting relevance of use of counter-surveillance techniques while driving); Bernard, 623 F.2d at 559-60 (considering defendants' counter-surveillance activities near drug laboratory). The use of public, rather than private, telephones is typical of narcotics traffickers and may be taken into account in evaluating probable cause. See Hoyos, 892 F.2d at 1393. Of course, a confidential informant's tip also figures into the determination of whether probable cause existed. See, e.g., Rodriguez, 869 F.2d at 482-83 (considering tips in determining probable cause). United States v. Roberts, 747 F.2d 537, 544 (9th Cir. 1984) (tip which could not establish probable cause by itself contributes to finding of probable cause). Another circuit has noted "the practice followed by some drug dealers of hiding" until the deal is consummated so that they can claim to be innocent bystanders in the event of governmental interference in the transaction. See United States v. Ashcroft, 607 F.2d 1167, 1171 (5th Cir. 1979), cert. denied, 446 U.S. 966, 100 S.Ct. 2944, 64 L.Ed.2d 826 (1980).

In considering whether the investigating officers here had probable cause to believe that Del Vizo was participating or had participated in the commission of a crime, we are not swayed by the presence or absence of any particular observation alone. Rather, we are impressed by the wealth of information gathered by the officers and the extent to which that information revealed a "pattern of activity" indicating participation in a narcotics transaction. See United States v. Espinosa, 827 F.2d 604, 610 (9th Cir. 1987) (following tip, officers observed pattern of activity consistent with participation in a drug ring), cert. denied, 485 U.S. 968, 108 S.Ct. 1243, 99 L.Ed.2d 441 (1988). It is of no moment that the facts of Del Vizo and his confederates, if viewed separately, might be consistent with innocence: "Conduct innocent in the eyes of the untrained may carry entirely different 'messages' to the experienced or trained observer." Bernard, 623 F.2d at 560 (quotation omitted). Although the question is a close one, under all of the circumstances, we are satisfied there was sufficient information to warrant a prudent person's belief that Del Vizo was involved in a narcotics transaction.

For these reasons, we conclude that Del Vizo's arrest was supported by probable cause.

IV

Our conclusion that Del Vizo's arrest prior to the search of his van was constitutional disposes of the other issues raised on appeal. The district court correctly denied Del Vizo's motion to suppress.
evidence.

AFFIRMED.

Footnotes

[ Footnote 1 ] Searches of various residences and vehicles of the conspirators yielded additional evidence, including cocaine, ledgers, and $186,000 in cash.


[ Footnote 4 ] We note that the district court engaged in the oft-criticized practice of adopting wholesale the findings and conclusions drafted by the prevailing party. "Indeed, the court merely crossed out the word 'proposed' in entering the challenged findings." Alvernaz Farms, Inc. v. Bank of California (In re T.H. Richards Processing Co.), 910 F.2d 639, 643 n. 2 (9th Cir. 1990). Hence we will review the district court's dual theories justifying the arrest with special scrutiny. See id., Sealy, Inc. v. Easy Living, Inc., 743 F.2d 1378, 1385 n. 3 (9th Cir. 1984) (same).

[ Footnote 5 ] We review de novo the district court's conclusion that there was no arrest prior to the discovery of cocaine. See United States v. Buffington, 815 F.2d 1292, 1300 (9th Cir. 1987). As noted previously, we apply special scrutiny. See supra note 4.

[ Footnote 6 ] We review de novo the district court's determination of probable cause. See Delgadillo-Velasquez, 856 F.2d at 1295. Again, special scrutiny is necessary. See supra note 4.

[ Footnote 7 ] In determining whether there was probable cause to arrest Del Vizo, the police were not limited to considering only Del Vizo's observed activities. Of course, a person's mere proximity to others engaged in criminal activity is insufficient to establish probable cause to search or arrest that person. See, e.g., Ybarra v. Illinois, 444 U.S. 85, 90-92, 100 S.Ct. 338, 341-43, 62 L.Ed.2d 238 (1979) (probable cause to search a tavern and a particular bartender due to the bartender's alleged involvement in narcotics did not justifiy the warrantless search of patrons of the bar who were in no way connected with the supposed drug-dealing); United States v. Robertson, 833 F.2d 777, 782 -83 (9th Cir. 1987) (a woman's mere presence on the grounds of an alleged drug laboratory was insufficient for probable cause to arrest her); cf. United States v. Vaughan, 718 F.2d 332, 334 (9th Cir. 1983) (mere presence in vehicle with two persons for whom the police possessed arrest warrants did not give rise to probable cause; "the agents were not aware of any involvement by him in the conspiracy ". [F]or all the agents knew at the time they detained Vaughan and searched his briefcase, he could have been a hitchhiker.").

However, where the police's observations give them a reasonable belief that the observed person is a part of the criminal enterprise, then the probable cause to arrest will extend to him as well. See, e.g., United States v. Rodriguez, 869 F.2d 479, 481 -83 (9th Cir. 1989) (where there was probable cause to arrest ring-leader of narcotics gang, there was also probable cause to arrest two men who took delivery of a van with large boxes inside; "[t]hey were seen as participants in a chain of conduct that was considered by the police to be an ongoing criminal operation"); United States v. Hillison, 733 F.2d 692, 697 -98 (9th Cir. 1984) (after two known drug dealers were arrested with cocaine, there was probable
cause to arrest man who was observed staying near and meeting with both); United States v Lomas, 706 F.2d 886, 892 (9th Cir. 1983) (where there was probable cause to arrest participants in sting operation, two suspicious-looking types who were apparently standing lookout could be arrested as well), cert. denied, 464 U.S. 1047, 104 S.Ct. 720, 79 L.Ed.2d 182 (1984). We have no difficulty concluding that Del Vizo's observed conduct was sufficient for the police reasonably to infer participation in the criminal enterprise. See Hillison, 733 F.2d at 697. The police had certainly seen enough to know that Del Vizo was not some "innocent visitor," see Robertson, 833 F.2d at 782, or "a hitchhiker," see Vaughan, 718 F.2d at 334.

[Footnote 8] See also United States v Leon, 460 F.2d 299 (9th Cir. 1972). In Leon, border officials knew that they were in a prime smuggling area, that defendant had rented an automobile and motel room, and that defendant was a suspected narcotics dealer. These officials had probable cause to arrest when they had observed a nighttime meeting with a foreigner, after which suspects were seen with loaded bags and foil-wrapped items. Id. at 300. Similarly, in this case the officers had been tipped that narcotics activity centered around the Ashworth residence and had observed activity which closely matched the profile of a drug transaction with vehicle switches, meetings, a point man, counter-surveillance measures, and mysterious packages.

[Footnote 9] Del Vizo asserts that his on-site consent to a search of the van was tainted by his illegal arrest. However, because the arrest was not illegal, the admitted consent carries no taint. Del Vizo's contention that the warrants for subsequent searches of various residences were defective, in that they were based upon the discovery of cocaine in Del Vizo's van during the purportedly illegal search, is meritless for the same reason.
THE HONORABLE ROBERT J. KOCHLY, DISTRICT ATTORNEY, COUNTY OF CONTRA COSTA, has requested an opinion on the following questions:

1. Do the federal statutes governing the installation of pen registers and trap and trace devices provide authority for issuance of a state court order permitting a state law enforcement officer to install or use pen registers or trap and trace devices?

2. Do the state statutes governing the issuance of administrative subpoenas provide authority for a state law enforcement officer to install or use pen registers or trap and trace devices?
CONCLUSIONS

1. The federal statutes governing the installation of pen registers and trap and trace devices do not provide authority for issuance of a state court order permitting a state law enforcement officer to install or use pen registers or trap and trace devices.

2. The state statutes governing the issuance of administrative subpoenas do not provide authority for a state law enforcement officer to install or use pen registers or trap and trace devices.

ANALYSIS

A “pen register” records the numbers dialed out from a particular telephone line. (Smith v. Maryland (1979) 442 U.S. 735, 736, fn. 1; People v. Blair (1979) 25 Cal.3d 640, 654, fn. 11.) A “trap and trace device” records the originating telephone numbers of the calls dialed into a particular telephone line. (People v. Suite (1980) 101 Cal.App.3d 680, 684.)¹ The placement of pen registers and trap and trace devices allows law enforcement officers to obtain such information as the names of suspects in an investigation, the identities and relationship between individuals suspected of engaging in criminal activity, especially in conspiracies, and the location of fugitives.

Search warrants issued by a court and subpoenas issued either by a court or grand jury are normally available to authorize the placement of pen registers and trap and trace devices in California.² The two questions presented for resolution concern whether federal statutes governing the installation of pen registers and trap and trace devices and state statutes governing the issuance of administrative subpoenas may also provide authority for state law enforcement officers to obtain telephone calling records. We conclude that these two additional sources of authority are not available to state law enforcement officers in the circumstances presented.

¹ Pen registers and trap and trace devices are not “wiretaps,” that is, they do not eavesdrop on or record telephone conversations. (Smith v. Maryland, supra, 442 U.S. at p. 736, fn. 1, People v. Blair, supra, 25 Cal.3d at p. 654, fn. 11, 69 Ops.Cal.Atty.Gen. 55, 58 (1986).) Generally speaking, the legal requirements for placing a wiretap are more stringent than those for placing a pen register or trap and trace device. (69 Ops.Cal.Atty.Gen, supra; at pp. 56-58.)

² Law enforcement officers may also procure telephone calling information by obtaining the person’s consent or if “exigent circumstances” are present. (See, e.g., People v. Chapman (1984) 36 Cal.3d 981, 113; People v. Suite, supra, 101 Cal.App.3d at p. 687.)
1. Federal Statutes

The Fourth Amendment to the United States Constitution guarantees "[t]he right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures." To determine whether a particular form of governmental surveillance is a "search" within the meaning of the Fourth Amendment, courts generally look to the leading case of Katz v. United States (1967) 389 U.S. 347, which involved eavesdropping by means of an electronic listening device placed on the outside of a telephone booth. (See, e.g., Kyllo v. United States (2001) 533 U.S. 27, 32-33.) In Katz, the court held that the eavesdropping in question constituted an unlawful search because it violated a subjective expectation of privacy that society recognized as reasonable. (Katz v. United States, supra, 389 U.S. at p. 353.)

In Smith v. Maryland, supra, 442 U.S. 735, the court followed the Katz standard, concluding that individuals have no Fourth Amendment expectation of privacy in the numbers dialed to or from their telephone lines. The court reasoned that telephone customers are generally aware that telephone companies routinely collect and use such information for various purposes including billing and system maintenance.

In 1986, following the Smith decision, Congress enacted a statutory scheme (18 U.S.C. §§ 3121-3127) regulating the use of pen registers and trap and trace devices. As relevant for our purposes, section 3121 provides:

"(a) Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title . . . ."

---

3 All references hereafter to title 18 of the United States Code prior to footnote 7 are by section number only.

4 The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act, Pub. L. No. 107-56) amended the definitions of "pen register" and "trap and trace device" to include processes that capture routing, addressing, or signaling information transmitted by an electronic communication facility. (18 U.S.C. § 3127 (3), (4).) These amendments permit government officials to obtain information from computers and cell phones as well as from land-line telephones. (See 18 U.S.C. § 3121.) Issues arising from these statutory amendments are beyond the scope of this opinion.
Section 3122 states:

“(a)(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

“(b) An application under subsection (a) of this section shall include

“(1) the identity of ... the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

“(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.”

Section 3123 provides:

“(a)(2) Upon an application made under section 3122 of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court if the court finds that ... the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

“(d) An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that

“(1) the order be sealed until otherwise ordered by the court; and

“(2) the person owning or leasing the line to which the pen register
or trap and trace device is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.”

Thus, as a general rule, federal law forbids the use of pen registers and trap and trace devices without the consent of the telephone consumer or a court order. (§ 3121.) Significantly, the federal statutes do not allow state law enforcement officers to apply for a state court order if the order would be "prohibited by State law." (§ 3122(a)(2).) Accordingly, we must look to California law to determine if the federal statutes may provide authority for state law enforcement officers to obtain telephone calling records in the circumstances presented.5

The California Constitution is a “document of independent force” (American Academy of Pediatrics v. Lungren (1997) 16 Cal.4th 307, 325), which extends protection for civil rights broader than and independent of the parallel rights afforded by the United States Constitution. (Id. at pp. 325-326; see People v. Pettingill (1978) 21 Cal.3d 231, 247; People v. Hannon (1977) 19 Cal.3d 588, 606.) Section 13 of article I of the California Constitution protects “against unreasonable seizures and searches.”6 Our Supreme Court has held “that, in determining whether an illegal search has occurred under the provisions of our Constitution, the appropriate test is whether a person has exhibited a reasonable expectation of privacy and, if so, whether that expectation has been violated by unreasonable governmental intrusion.” (Burrows v. Superior Court (1974) 13 Cal.3d 238, 242-243.) In Burrows, the court concluded that bank customers have a reasonable expectation of privacy in the financial information they transmit to their banks; reasoning that it is impossible to participate in the economic life of contemporary society without maintaining a bank account and that the totality of a person’s bank records provides a “virtual current biography.” (Id. at p. 247.)

5 We recognize that the California Constitution eliminates any judicially created independent state grounds for the exclusion of evidence. (Cal. Const., art. I, § 28, subd. (d); In re Lance W (1985) 37 Cal.3d 873, 886-887.) As a result, telephone calling records would be admissible against a California defendant in a criminal trial even though their seizure violated the California Constitution, as long as the records were admissible under the federal Constitution. (See, e.g., People v. Bencomo (1985) 171 Cal.App.3d 1005, 1015; People v. Lissauer (1985) 169 Cal.App.3d 413, 419.) Regardless of the evidence’s admissibility, however, the underlying act of seizure in violation of the California Constitution would remain unlawful. (In re Lance W., supra, 37 Cal.3d at p. 886; People v. Martino (1985) 166 Cal.App.3d 777, 785, fn. 3.)

6 “The right of the people to be secure in their persons, houses, papers, and effects against unreasonable seizures and searches may not be violated.” (Cal. Const., art. I, § 13.)
In People v. Blair, supra, 25 Cal.3d 640, the court rejected the rationale of Smith v. Maryland, supra, 442 U.S. 735, and concluded that telephone records, like the bank records found protected under California law in Burrows v. Superior Court, supra, 13 Cal.3d 238, were protected against unreasonable searches and seizures in California. (Id. at p. 653.) In Blair, the telephone records were obtained by a subpoena issued by a Federal Bureau of Investigation agent under authority of a United States Attorney as authorized by a federal grand jury. The court found that the federal subpoena was insufficient for purposes of the search and seizure provisions of the California Constitution since there had been no prior “judicial determination that law enforcement officials were entitled” to the records. (Id. at p. 655; see Carlson v. Superior Court (1976) 58 Cal.App.3d 13, 21-23.) Consequently, the seizure of the telephone records was ruled a violation of article I, section 13 of the California Constitution.

We believe that telephone calling records would additionally be protected under article I, section 1 of the California Constitution, which provides:

“All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.”

Under the rationale of Burrows and Blair, information obtained from pen registers and trap and trace devices would fall within the zone of privacy protected by the state Constitution, since the records of incoming or outgoing calls could lead to the discovery of an individual’s “virtual current biography.” (People v. Blair, supra, 25 Cal.3d at p. 653; Burrows v. Superior Court, supra, 13 Cal.3d at p. 247; People v. Chapman, supra, 36 Cal.3d at p. 109.)

Based upon the foregoing, we find that the California Constitution allows the placement of pen registers and trap and trace devices only if a judicial ruling is first obtained that the law enforcement officers are entitled to the records. (See 69 Ops.Cal.Atty.Gen., supra, at p. 59.) Do the court procedures set forth in federal law meet this state constitutional standard for prior judicial review? They do not.

The federal statutory scheme permits state law enforcement officers to apply for a state court order authorizing the use of a pen register or trap and trace device based upon a written certification that the information is “relevant to an ongoing criminal investigation.” (18 U.S.C. § 3122(b)(2).) Upon a proper application, the court must issue the order. (18 U.S.C. § 3122(a)(2).) The statutes do not authorize a court to go outside the written certification (In re Order Authorizing Installation of Pen Reg. (M.D.Fla. 1994) 846 03-406 - 3877 -
F.Supp. 1555, 1559), thus making the judicial review "ministerial in nature" (United States v. Fregoso (8th Cir. 1995) 60 F.3d 1314, 1320).

Under Burrows and Blair, this federal statutory process is inadequate to protect a California resident's privacy interests in telephone calling records. As previously noted, the federal subpoena in Blair was found not to constitute appropriate "legal process" because issuance of the subpoena was a ministerial act with no "judicial determination" that the issuer was "entitled" to obtain the information. (People v. Blair, supra, 25 Cal.3d at pp. 651, 655.) A seizure of information is unreasonable when "the character, scope, and relevancy of the material obtained were determined entirely by the exercise of the unbridled discretion of the police." (People v. Chapman, supra, 36 Cal.3d at p. 113, quoting Burrows v. Superior Court, supra, 13 Cal.3d at p. 243; see People v. Blair, supra, 25 Cal.3d at p. 651.)

The federal statutes governing pen registers and trap and trace devices likewise fail the California constitutional test. No adequate prior judicial review is provided in the statutory scheme; rather, unbridled discretion is given to law enforcement officers.

We conclude in answer to the first question that the federal statutes governing the installation of pen registers and trap and trace devices do not provide authority for issuance of a state court order permitting a state law enforcement officer to install or use pen registers or trap and trace devices.

2. State Administrative Subpoena Statutes

Government Code section 11180 authorizes the head of each of the state's departments to conduct investigations concerning matters relating to the subjects under the department's jurisdiction. Included within this power is the right to subpoena records. (§ 11181, subd. (e).) The department head may delegate subpoena powers to any officer of the department authorized to conduct the investigation. (§ 11182.)

Significantly, the department head or designee may issue a subpoena for investigative purposes in the absence of any formal charge or court proceeding. (§§ 11180, 11181; Brovelli v. Superior Court (1961) 56 Cal.2d 524, 527-528.) The subpoenas are returnable directly to the department head, and no provision is made for notice to a third party—such as a telephone customer—or for the filing of a motion to quash or other formal opposition. (Compare §§ 11181, 11184, 11187 with Pen. Code, §§ 03-406)
Instead, if the subpoenaed party fails to comply with the subpoena, the department head may apply to a court for an order enforcing the subpoena. (§ 11187.) If it appears at the hearing “that the subpoena was regularly issued ... the court shall enter an order” enforcing the subpoena. (§ 11188, italics added.) Hence, judicial enforcement of administrative subpoenas is subject to a standard less exacting than that required for a criminal search warrant. (See Craib v. Bulmash (1989) 49 Cal.3d 475, 481-486.)

Of course, “department heads cannot compel the production of evidence in disregard of ... the constitutional provisions prohibiting unreasonable searches and seizures.” (Brovelli v. Superior Court, supra, 56 Cal.2d at p. 529; see also Pacific-Union Club v. Superior Court (1991) 232 Cal.App.3d 60, 70, 79-80; Wood v. Superior Court (1985) 166 Cal.App.3d 1138, 1146-1147.) “[A] governmental administrative agency is not in a special or privileged category, exempt from the right of privacy requirements which must be met and honored generally by law enforcement officials.” (Board of Medical Quality Assurance v. Gherardini (1979) 93 Cal.App.3d 669, 679-680; see Carlson v. Superior Court, supra, 58 Cal.App.3d at p. 22 [“Surely an accused’s constitutional right to privacy in his papers and records is not diminished because law enforcement officials seek to obtain them by subpoena rather than by warrant”].)

As with the federal statutes governing the installation of pen registers and trap and trace devices, the state administrative subpoena statutes do not contain a provision allowing for prior judicial review establishing that the law enforcement officers are entitled to the records. The California Constitution requires such prior review.

We conclude in answer to the second question that the state statutes governing the issuance of administrative subpoenas do not provide authority for a state law enforcement officer to install or use pen registers or trap and trace devices.

*****
Specialized Surveillance Equipment & Techniques

Supplemental Handouts
§ 1524.2. Definitions; Warrant for search of records of foreign corporation providing electronic communication or remote computing services; Records revealing specified information about customers; California corporation served with warrant issued by another state

(a) As used in this section, the following terms have the following meanings:

(1) The terms "electronic communication services" and "remote computing services" shall be construed in accordance with the Electronic Communications Privacy Act in Chapter 121 (commencing with Section 2701) of Part I of Title 18 of the United State Code Annotated. This section shall not apply to corporations that do not provide those services to the general public.

(2) An "adverse result" occurs when notification of the existence of a search warrant results in:

(A) Danger to the life or physical safety of an individual.

(B) A flight from prosecution.

(C) The destruction of or tampering with evidence.

(D) The intimidation of potential witnesses.

(E) Serious jeopardy to an investigation or undue delay of a trial.

(3) "Applicant" refers to the peace officer to whom a search warrant is issued pursuant to subdivision (a) of Section 1528.

(4) "California corporation" refers to any corporation or other entity that is subject to Section 102 of the Corporations Code, excluding foreign corporations.

(5) "Foreign corporation" refers to any corporation that is qualified to do business in this state pursuant to Section 2105 of the Corporations Code.

(6) "Properly served" means that a search warrant has been delivered by hand, or in a manner reasonably allowing for proof of delivery if delivered by United States mail, overnight delivery service, or facsimile to a person or entity listed in Section 2110 of the Corporations Code.

(b) The following provisions shall apply to any search warrant issued pursuant to this chapter allowing a search for records that are in the actual or constructive possession of a foreign corporation that provides electronic communication services or remote computing services to the general public, where those records would reveal the identity of the customers using those services, data stored by, or on behalf of, the customer, the customer's usage of those services, the recipient or destination of communications sent to or from those customers, or the content of those communications.

(1) When properly served with a search warrant issued by the California court, a foreign corporation subject to this section shall provide to the applicant, all records sought pursuant to that warrant within five business days of receipt, including those records maintained or located outside this state.

(2) Where the applicant makes a showing and the magistrate finds that failure to produce records within less than five business days would cause an adverse result, the warrant may require production of records within less than five business days. A court may reasonably extend the time required for production of the records upon finding that the foreign corporation has shown good cause for that extension and that an extension of time would not cause an adverse result.
(3) A foreign corporation seeking to quash the warrant must seek relief from the court that issued the warrant within the time required for production of records pursuant to this section. The issuing court shall hear and decide that motion no later than five court days after the motion is filed.

(4) The foreign corporation shall verify the authenticity of records that it produces by providing an affidavit that complies with the requirements set forth in Section 1561 of the Evidence Code. Those records shall be admissible in evidence as set forth in Section 1562 of the Evidence Code.

(c) A California corporation that provides electronic communication services or remote computing services to the general public, when served with a warrant issued by another state to produce records that would reveal the identity of the customers using those services, data stored by, or on behalf of, the customer, the customer's usage of those services, the recipient or destination of communications sent to or from those customers, or the content of those communications, shall produce those records as if that warrant had been issued by a California court.

(d) No cause of action shall lie against any foreign or California corporation subject to this section, its officers, employees, agents, or other specified persons for providing records, information, facilities, or assistance in accordance with the terms of a warrant issued pursuant to this chapter.

HISTORY:
 Added Stats 1999 ch 896 § 2 (SB 662).
Assembly Bill No. 1305

CHAPTER 17

An act to amend Section 629.51 of the Penal Code, relating to wiretaps.

[Approved by Governor June 22, 2005. Filed with Secretary of State June 22, 2005.]

LEGISLATIVE COUNSEL'S DIGEST

AB 1305, Sharon Runner. Wiretaps.
Existing law defines "wire communication" as any transfer of the human voice made with the aid of specified connections between the point of origin and point of reception, furnished by specified persons or facilities. The definition also includes the electronic storage of these communications.

This bill would delete storage of these communications from the definition.

The people of the State of California do enact as follows:

SECTION 1. Section 629.51 of the Penal Code is amended to read:

629.51. For the purposes of this chapter, the following terms have the following meanings:

(a) "Wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of a like connection in a switching station), furnished or operated by any person engaged in providing or operating these facilities for the transmission of communications.

(b) "Electronic pager communication" means any tone or digital display or tone and voice pager communication.

(c) "Electronic cellular telephone communication" means any cellular or cordless radio telephone communication.

(d) "Aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception.
AB 1305 Assembly Bill - Bill Analysis

SENATE COMMITTEE ON PUBLIC SAFETY
Senator Elaine K. Alquist, Chair
2005-2006 Regular Session

AB 1305 (Sharon Runner)
As Introduced February 22, 2005
Hearing date: June 7, 2005
Penal Code
MK:br

WIRETAPS

HISTORY

Source: Los Angeles District Attorney's Office

Prior Legislation: SB 32 (McPherson) -2003; not heard in Senate Public Safety Committee
AB 74 (Washington) -Ch. 605, Stats. 2002
SB 662 (Figuerca) - Ch. 896, Stats. 1999

Support: California District Attorneys Association; California Peace Officers' Association; Office of the Attorney General

Opposition: None known

Assembly Floor Vote: Ayes 74 - Noes 0

KEY ISSUE

SHOULD THE DEFINITION OF WIRE COMMUNICATION IN THE WIRETAP PROVISIONS BE AMENDED TO MAKE IT CLEAR THAT IT DOES NOT INCLUDE "STORED COMMUNICATIONS"?

(More)
PURPOSE

The purpose of this bill is to clarify that the wiretap provisions do not apply to voice mail and other stored communications.

Existing law allows for the intercept of wire communications by law enforcement under specified circumstances. (Penal Code 629.50 et. seq.)

Existing law includes in the definition of "wire communications" any electronic storage of specified communications. (Penal Code 629.51.)

This bill deletes the reference to the "electronic storage" of the communications.

(More)
1. Need for This Bill

According to the author:

Existing law includes electronically stored communications (voice mail) within the definition of a wire communication. This definition was a result of a drafting error in AB 74 (Washington), Chapter 605, Statutes of 2002. When references to stored communications were removed from AB 74, the term was inadvertently retained as part of the definition of "wire communication". This bill would remove that language that designates voice mail as a type of telephone communication that requires a wiretap authorization before the stored messages can be retrieved by law enforcement.

2. Background

According to the sponsor:

As part of the negotiations of AB 74, it was agreed by law enforcement, prosecutors, representatives of the defense bar and privacy advocates that California's wiretap statute should only apply to wire communications between the point of origin and the point of reception. References to 'stored communications' were removed from AB 74 because law enforcement has the authority to obtain stored communications by means of a search warrant under Penal Code Section 1524.2. When references to 'stored communications' were removed from AB 74, the term was inadvertently retained as part of the definition of wire communication.

This bill would remove 'stored communications' from the definition of 'wire communications' and instead would require the contents of voice mail and other stored communications be obtained through a search warrant.

California enacted Penal Code Section 1524.2(b), which specifically permits the acquisition of the contents of voicemail and other stored communications (e.g., e-mail) through search warrants. Penal Code...
Section 1524.2(b) states in pertinent part:

The following provisions shall apply to any search warrant issued pursuant to this chapter allowing a search for records that are in the actual or constructive possession of a foreign corporation that provides electronic communication services or remote computing services to the general public, where those records would reveal the identity of the customers using those services, data stored by, or on behalf of, the customer, the customer's usage of those services, the recipient or destination of communications sent to or from those customers, or the content of those communications.

The issue of whether a search warrant is required for stored voice mail has been litigated in at least two California counties under the new (AB 74) California wiretap law. As noted in the article, 'Searching E-Mail and Voicemail', that appeared in the Winter 2003 issue of the Alameda County District Attorney's Office publication "Point of View", Footnote #5 states:

NOTE: To say that the law has been cleared up does not necessarily mean that there will be an end to such litigation. In September 2002, AT&T Wireless filed a motion to quash a warrant for voicemail obtained by Hayward homicide detectives on grounds a wiretap order was required under Penal Code Section 629.50 et seq. The motion was baseless and was denied. In October 2002, AT&T Wireless filed an identical motion to quash a search warrant in Santa Clara County. Although AT&T Wireless claims it filed the motions only because it feared it might incur civil liability for providing voicemail without full wiretap authorization, AT&T Wireless and other providers of voicemail who furnish copies of voicemail messages pursuant to a search warrant are, in fact, immune from civil liability pursuant to Penal Code Section 1524.2(d).
3. **Deletion of "Stored Communications"**

By deleting "any electronic storage of these communications" from the definition of "wire communications" this bill clarifies that voice mail and other stored communications are obtainable by search warrant and a wiretap order is not necessary for these communications. As noted above this is consistent with what was intended by the most recent amendments to the wiretap provisions made by AB 74 (Washington) Chapter 605, Stats. 2002.

***************
Date of Hearing: May 3, 2005
Counsel. Kimberly Horluch

ASSEMBLY COMMITTEE ON PUBLIC SAFETY
Mark Leno, Chair

AB 1305 (Runner) - As Introduced: February 22, 2005

SUMMARY: Deletes from the definition of "wire communication" the inclusion of "any electronic storage" of wire communications.

EXISTING LAW:

1) Authorizes the Attorney General, chief deputy attorney general, chief assistant attorney general, or district attorney to apply to the presiding judge of the superior court for an order authorizing the interception of wire, electronic digital pager, or electronic cellular telephone communications under specified circumstances. (Penal Code Section 629.50.)

2) Specifies the crimes for which an interception order may be sought: murder; kidnapping; bombing; criminal gangs; and possession for sale; and sale, transportation, or manufacturing of more than three pounds of cocaine, heroin, PCP, or methamphetamine. (Penal Code Section 629.52.)

3) Provides that the court may grant oral approval for an emergency interception without an order as specified. Approval for an oral interception shall be conditioned upon filing with the court, within 48 hours of the oral approval, a written application for an order. (Penal Code Section 629.56.)

4) Requires that written reports be submitted at least every 72 hours to the judge who issued the order allowing the interception. (Penal Code Section 629.60.)

5) Provides that before evidence derived from an intercepted communication may be received in evidence, each party must be given a copy of the transcript of the contents of the interception and a copy of the court order 10 days before any court proceeding, except as otherwise specified. (Penal Code
Section 629.70.

6) Provides that any person may move to suppress intercepted communications on the basis that the contents or evidence were obtained in violation of the Fourth Amendment to the United States Constitution or of California electronic surveillance provisions. (Penal Code Section 629.72.)

7) Provides that if a law enforcement officer overhears a communication relating to a crime that is not specified in the wiretap order, but is a crime for which a wiretap order could have been issued, the officer may only disclose the information and thereafter use the evidence, if, as soon as practical, he or she applies to the court for permission to use the information. If an officer overhears a communication relating to a crime that is not specified in the order, and not one for which a wiretap order could have been issued, the information may not be disclosed or used except to prevent the commission of a crime. No evidence derived from the wiretap can be used unless the officers can establish that the evidence was obtained through an independent source or inevitably would have been discovered. In all instances, the court may only authorize use of the information if it reviews the procedures used and determines that the interception was in accordance with state wiretap laws. [Penal Code Section 629.82(b)].

8) Prohibits the covert entry into a residential dwelling, hotel, or motel room for installation or removal of any interception device or for any other purpose. Covert entry to facilitate an order to intercept communications is prohibited by the provisions of wiretap provisions. (Penal Code Section 629.89.)

FISCAL EFFECT: Unknown

COMMENTS:

1) Author's Statement: According to the author, "Existing law includes electronically stored communications (voice mail) within the definition of a wire communication. This definition was a result of a drafting error in AB 74 (Washington), Chapter 605, Statutes of 2002. When references to stored communications were removed from AB 74, the term was inadvertently retained as part of the definition of 'wire communication'. This bill would remove that language that
designates voice mail as a type of telephone communication that requires a wiretap authorization before the stored messages can be retrieved by law enforcement."

2) **Background**: According to background provided by the author, "Existing law includes communications left on voice mail (i.e., "electronic storage of these communications") as a type of telephone communication that requires a wiretap authorization before the stored messages can be retrieved by law enforcement. This definition was the result of a drafting error in AB 74. AB 74 extended the sunset of California's wiretap law and made other changes that were mutually agreed upon by law enforcement, prosecutors, representatives of the defense bar and privacy advocates.

"As part of the negotiations of AB 74, it was agreed by law enforcement, prosecutors, representatives of the defense bar and privacy advocates that California's wiretap statute should only apply to wire communications between the point of origin and the point of reception. References to 'stored communications' were removed from AB 74 because law enforcement has the authority to obtain stored communications by means of a search warrant under Penal Code Section 1524.2. When references to 'stored communications' were removed from AB 74, the term was inadvertently retained as part of the definition of wire communication.

"This bill would remove 'stored communications' from the definition of 'wire communications' and instead would require the contents of voice mail and other stored communications be obtained through a search warrant."

"California enacted Penal Code Section 1524.2(b), which specifically permits the acquisition of the contents of voicemail and other stored communications (e.g., e-mail) through search warrants. Penal Code Section 1524.2(b) states in pertinent part:

'The following provisions shall apply to any search warrant issued pursuant to this chapter allowing a search for records that are in the actual or constructive possession of a foreign corporation that provides electronic communication services or remote computing services to the general public, where those records would reveal the identity of the customers using those services, data stored by, or on behalf of, the customer, the customer's usage of those services, the recipient or destination of communications sent to or from those customers, or the content of those communications.'
"The issue of whether a search warrant is required for stored voice mail has been litigated in at least two California counties under the new (AB 74) California wiretap law. As noted in the article, 'Searching E-Mail and Voicemail', that appeared in the Winter 2003 issue of the Alameda County District Attorney's Office publication "Point of View", Footnote #5 states:

'NOTE: To say that the law has been cleared up does not necessarily mean that there will be an end to such litigation. In September 2002, AT&T Wireless filed a motion to quash a warrant for voicemail obtained by Hayward homicide detectives on grounds a wiretap order was required under Penal Code Section 629.50 et seq. The motion was baseless and was denied. In October 2002, AT&T Wireless filed an identical motion to quash a search warrant in Santa Clara County. Although AT&T Wireless claims it filed the motions only because it feared it might incur civil liability for providing voicemail without full wiretap authorization, AT&T Wireless and other providers of voicemail who furnish copies of voicemail messages pursuant to a search warrant are, in fact, immune from civil liability pursuant to Penal Code Section 1524.2(d)'."

3) Background - Federal Wiretapping Law:

a) The Fourth Amendment Protects Telephone Communications

The United States Supreme Court ruled in Katz v. United States (1967) 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2D 576, that telephone conversations were protected by the Fourth Amendment to the United States Constitution. Intercepting a conversation is a search and seizure similar to the search of a citizen's home. Thus, law enforcement is constitutionally required to obtain a warrant based on probable cause and to give notice and inventory of the search.

b) Title III Allows Wiretapping under Strict Conditions

In 1968, Congress authorized wiretapping by enacting Title III of the Omnibus Crime Control and Safe Streets Act.

(See 18 USC Section 2510 et seq.) Out of concern that telephonic interceptions do not limit the search and seizure to only the party named in the warrant, federal law prohibits electronic surveillance except under carefully defined circumstances. The procedural steps provided in the Act require "strict adherence." [United States v. Kalustian, 523 F.2d 585, 588 (9th Cir. 1976), and "utmost scrutiny must be exercised to determine whether wiretap orders conform to Title III." Several of the relevant
Statutory requirements may be summarized as follows:

i) Unlawfully intercepted communications or non-conformity with the order of authorization may result in the suppression of evidence.

ii) Civil and criminal penalties for statutory violations.

iii) Wiretapping is limited to enumerated serious felonies.

iv) Only the highest ranking prosecutor may apply for a wiretap order.

v) Notice and inventory of a wiretap shall be served on specified persons within a reasonable time but not later than 90 days after the expiration of the order or denial of the application.

vi) Judges are required to report each individual interception. Prosecutors are required to report interceptions and statistics to allow public monitoring of government wiretapping.

c) The Necessity Requirement - Have Other Investigative Techniques Been Tried Before Applying to the Court for a Wiretap Order - Both federal and California law require that each wiretap application include "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." [18 USC Section 2518 (1)(c); Penal Code Section 629.50(d).] Often referred to as the "necessity requirement", it exists in order to limit the use of wiretaps, which are highly intrusive. [United States v.

Bennett, 219 F.3d 1117, 1121 (9th Cir. 2000).] The original intent of Congress in enacting such a provision was to ensure that wiretapping was not resorted to in situations where traditional investigative techniques would suffice to expose the crime.

The United States Court of Appeals for the Ninth Circuit recently suppressed wiretap evidence against a defendant and reversed his conviction for failure of the government to make a showing of necessity for the electronic monitoring. Purged of material omissions and misstatements, the Court held that the application failed to contain sufficiently specific facts to satisfy the

1) Comparison of California to Federal Law:

a) Title III Sets Minimum Standards for the States to Follow – Title III mandates that before any state law enforcement officers may use wiretaps, the state must pass an enabling statute which, at a minimum, affords the same protections as the federal law. [18 U.S.C. 2516(2); People v. Chavez (1996) 44 Cal.App.4th 1144, 1150; People v. Otto (1992) 2 Cal.4th 1088, 1092, fn. 1, 1098; Bunnell v. Superior Court (1994) 21 Cal.App.4th 1811, 1818.]

b) Broader Standing – Who May Challenge the Legality of an Interception Order – Under federal law, only an "aggrieved person" has standing to move to suppress derivative evidence. (18 USC Section 2518.) A defendant may seek to suppress all evidence derived from his or her own intercepted communications if he or she was named or otherwise identified in a wiretap order or owned the property from which such interceptions took place. [18 USC Section 2518(6)(d); Penal Code Section 629.66; Alderman v. United States (1969) 394 U.S. 165, 174, 89 S.Ct. 961, 966, 22 L.Ed.2d 176.] Under federal law, a defendant does not have standing to contest evidence that was derived from a third party's intercepted communication. There is no right under Federal law to assert the standing of a third party. [Alderman v. United States, supra, 394 U.S. 165, 176, 89 S.Ct. 961, 966, 22 L.Ed.2d 176.]

c) Broader Grounds for the Suppression of Evidence – California law has broader grounds for the suppression of evidence than federal law. Title III provides for the
remedy of suppression for evidence "unlawfully intercepted," derived from a facially invalid order, or resulting from non-conformity with the order. As mentioned previously, Penal Code Section 629.72 authorizes suppression for evidence "obtained in violation of the Fourth Amendment of the United States Constitution or of this chapter" (emphasis added).

d) Mandatory Notice and Inventory for Any Person Intercepted - Notice of a wiretap 90 days after the order expires is mandatory under the state law to all persons intercepted by a wiretap, rather than merely discretionary as provided by federal law. [18 U.S.C. Section 2518(8)(d); Penal Code Section 629.68.]

e) Civil and Criminal Liability for Law Enforcement Violations is Greater - Civil damages for any violation of the law is $100 per day, rather than the federal compulsory damage award of only $50 per day. [18 U.S.C. Sections 2520 and 2511(4); Penal Code Section Code 629.86(c).] Penal Code Section 629.84 provides that any violation of wiretap laws is punishable by an imprisonment in the county jail for one year or by imprisonment in the state prison.

f) Wiretaps May Only Be Used in Cases Involving Murder, Kidnapping, Bombing, Criminal Gangs, and Sale of More than Three Pounds of Cocaine, Heroin, PCP, or Methamphetamine - The suspected crimes for which a wiretap may be issued are severely more limited than the federal law. [18 U.S.C. 2516(2); Penal Code Section 629.52.]

g) More Limited Authority for Applying for Wiretaps - The authority for making a wiretap application to a judge is also more limited. Only the Attorney General, chief deputy attorney general, chief assistant attorney general, or district attorney may make such an application. Unlike federal law, that authority cannot be delegated to any other person. [18 U.S.C. 2516(1); Penal Code Section 629.52.] Moreover, that application must be made in writing under personal oath. (Penal Code Section 629.52.) Federal law requires that both the application and order be provided at least 10 days before any hearing, trial, or proceeding; the California law additionally requires that transcripts of all communications be provided as well. [18 U.S.C. 2518(9); Penal Code Section 629.70.] While under federal law any United States district court or court of appeal may issue a wiretap order, federal law only allows a state court of competent jurisdiction as authorized by statute to issue wiretap orders. Penal Code Section 629.50
only authorizes the presiding judge of a county, or his or
her designee, to issue wiretap orders; however, a recent
decision by the court of appeal permitted the sequential
designation of several judges who may consider wiretap
239.]

h) Both Disclosure and Use of Wiretap Information is
Limited to Enumerated Offenses - Federal law allows police
officers to disclose to other officers, and thereafter use
any evidence derived there from, almost any information
obtained from an intercepted communication. (18 U.S.C.
Section 2517.) However, California severely restricts both
disclosure and use of information derived from a wiretap,
as well as the authority of any court to authorize such
disclosure or use. Penal Code Section 629.82 sets forth
the following limitations:

1) If an officer overhears a communication relating to
a crime not specified in the wiretap order but is a crime
for which a wiretap order could have been issued, the
police may only disclose the information to another
officer and thereafter use the evidence if, as soon as
practical, they apply to the court for permission to use

the information. The issuing judge may only authorize
use of the information if he or she reviews the
procedures used and determines that the wiretap was in
accordance with state wiretap laws.

11) If an officer overhears a communication relating to
a crime not specified in the order and not one for which
a wiretap order could have been issued, the information
may not be disclosed or used except to prevent the
commission of a crime. No evidence derived from the
wiretap can be used unless the officers can establish
that the evidence was obtained through an independent
source or inevitably would have been discovered. Even
then, a judge may only authorize use of such evidence if
it reviews the procedures used and determines that the
wiretap was in accordance with state wiretap laws.

Moreover, if any intercepted communication is used to
obtain a search warrant, which would include a wiretap
order or an arrest warrant, the person named in the
warrant is entitled to notice of the wiretap and a copy
of the contents of all intercepted communications used.
[Penal Code Section 629.82(c).]

1) Prior Legislation : AB 74 (Washington), Chapter 605, Statutes
of 2002 extended the sunset date on the current wiretap law and revised existing provisions to reflect changes in communication technology.

**REGISTERED SUPPORT / OPPOSITION:**

**Support**

Los Angeles County District Attorney's Office (Sponsor)
California District Attorneys Association
Department of Justice

**Opposition**

None on file

__Analysis Prepared by__ : Kimberly Horiuchi / PUB. S. / (916) 319-3744
THE HONORABLE ROBERT J. KOCHLY, DISTRICT ATTORNEY, COUNTY OF CONTRA COSTA, has requested an opinion on the following questions:

1. Do the federal statutes governing the installation of pen registers and trap and trace devices provide authority for issuance of a state court order permitting a state law enforcement officer to install or use pen registers or trap and trace devices?

2. Do the state statutes governing the issuance of administrative subpoenas provide authority for a state law enforcement officer to install or use pen registers or trap and trace devices?
CONCLUSIONS

1. The federal statutes governing the installation of pen registers and trap and trace devices do not provide authority for issuance of a state court order permitting a state law enforcement officer to install or use pen registers or trap and trace devices.

2. The state statutes governing the issuance of administrative subpoenas do not provide authority for a state law enforcement officer to install or use pen registers or trap and trace devices.

ANALYSIS

A “pen register” records the numbers dialed out from a particular telephone line. (Smith v. Maryland (1979) 442 U.S. 735, 736, fn. 1; People v. Blair (1979) 25 Cal.3d 640, 654, fn. 11.) A “trap and trace device” records the originating telephone numbers of the calls dialed into a particular telephone line. (People v. Suite (1980) 101 Cal.App.3d 680, 684.) The placement of pen registers and trap and trace devices allows law enforcement officers to obtain such information as the names of suspects in an investigation, the identities and relationship between individuals suspected of engaging in criminal activity, especially in conspiracies, and the location of fugitives.

Search warrants issued by a court and subpoenas issued either by a court or grand jury are normally available to authorize the placement of pen registers and trap and trace devices in California. The two questions presented for resolution concern whether federal statutes governing the installation of pen registers and trap and trace devices and state statutes governing the issuance of administrative subpoenas may also provide authority for state law enforcement officers to obtain telephone calling records. We conclude that these two additional sources of authority are not available to state law enforcement officers in the circumstances presented.

---

1 Pen registers and trap and trace devices are not “wiretaps,” that is, they do not eavesdrop on or record telephone conversations. (Smith v. Maryland, supra, 442 U.S. at p. 736, fn. 1, People v. Blair, supra, 25 Cal.3d at p. 654, fn. 11, 69 Ops.Cal.Atty.Gen. 55, 58 (1986).) Generally speaking, the legal requirements for placing a wiretap are more stringent than those for placing a pen register or trap and trace device. (69 Ops.Cal.Atty.Gen, supra, at pp. 56-58.)

2 Law enforcement officers may also procure telephone calling information by obtaining the person’s consent or if “exigent circumstances” are present. (See, e.g., People v. Chapman (1984) 36 Cal.3d 981, 113; People v. Suite, supra, 101 Cal.App.3d at p. 687.)
1. Federal Statutes

The Fourth Amendment to the United States Constitution guarantees "[t]he right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures." To determine whether a particular form of governmental surveillance is a "search" within the meaning of the Fourth Amendment, courts generally look to the leading case of Katz v. United States (1967) 389 U.S. 347, which involved eavesdropping by means of an electronic listening device placed on the outside of a telephone booth. (See, e.g., Kyllo v. United States (2001) 533 U.S. 27, 32-33.) In Katz, the court held that the eavesdropping in question constituted an unlawful search because it violated a subjective expectation of privacy that society recognized as reasonable. (Katz v. United States, supra, 389 U.S. at p. 353.)

In Smith v. Maryland, supra, 442 U.S. 735, the court followed the Katz standard, concluding that individuals have no Fourth Amendment expectation of privacy in the numbers dialed to or from their telephone lines. The court reasoned that telephone customers are generally aware that telephone companies routinely collect and use such information for various purposes including billing and system maintenance.

In 1986, following the Smith decision, Congress enacted a statutory scheme (18 U.S.C. §§ 3121-3127)³ regulating the use of pen registers and trap and trace devices.⁴ As relevant for our purposes, section 3121 provides:

"(a) Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title . . . ."

³ All references hereafter to title 18 of the United States Code prior to footnote 7 are by section number only

⁴ The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act, Pub. L. No. 107-56) amended the definitions of "pen register" and "trap and trace device" to include processes that capture routing, addressing, or signaling information transmitted by an electronic communication facility. (18 U.S.C. § 3127 (3), (4).) These amendments permit government officials to obtain information from computers and cell phones as well as from land-line telephones. (See 18 U.S.C. § 3121.) Issues arising from these statutory amendments are beyond the scope of this opinion.
Section 3122 states:

"(a)(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

(b) An application under subsection (a) of this section shall include

(1) the identity of . . . the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."

Section 3123 provides:

"(a)(2) Upon an application made under section 3122 of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court if the court finds that . . . the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

(d) An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that

(1) the order be sealed until otherwise ordered by the court; and

(2) the person owning or leasing the line to which the pen register
or trap and trace device is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.”

Thus, as a general rule, federal law forbids the use of pen registers and trap and trace devices without the consent of the telephone consumer or a court order. (§ 3121.) Significantly, the federal statutes do not allow state law enforcement officers to apply for a state court order if the order would be “prohibited by State law.” (§ 3122(a)(2).) Accordingly, we must look to California law to determine if the federal statutes may provide authority for state law enforcement officers to obtain telephone calling records in the circumstances presented.5

The California Constitution is a “document of independent force” (American Academy of Pediatrics v. Lungren (1997) 16 Cal.4th 307, 325), which extends protection for civil rights broader than and independent of the parallel rights afforded by the United States Constitution. (Id. at pp. 325-326, see People v. Pettingill (1978) 21 Cal.3d 231, 247; People v. Hannon (1977) 19 Cal.3d 588, 606.) Section 13 of article I of the California Constitution protects “against unreasonable seizures and searches.”6 Our Supreme Court has held “that, in determining whether an illegal search has occurred under the provisions of our Constitution, the appropriate test is whether a person has exhibited a reasonable expectation of privacy and, if so, whether that expectation has been violated by unreasonable governmental intrusion.” (Burrows v. Superior Court (1974) 13 Cal.3d 238, 242-243.) In Burrows, the court concluded that bank customers have a reasonable expectation of privacy in the financial information they transmit to their banks, reasoning that it is impossible to participate in the economic life of contemporary society without maintaining a bank account and that the totality of a person’s bank records provides a “virtual current biography” (Id. at p. 247.)

5 We recognize that the California Constitution eliminates any judicially created independent state grounds for the exclusion of evidence. (Cal. Const., art. I, § 28, subd. (d); In re Lance W (1985) 37 Cal.3d 873, 886-887.) As a result, telephone calling records would be admissible against a California defendant in a criminal trial even though their seizure violated the California Constitution, as long as the records were admissible under the federal Constitution. (See, e.g., People v. Bencomo (1985) 171 Cal.App.3d 1005, 1015; People v. Lissauer (1985) 169 Cal.App.3d 413, 419.) Regardless of the evidence’s admissibility, however, the underlying act of seizure in violation of the California Constitution would remain unlawful. (In re Lance W., supra.)

6 “The right of the people to be secure in their persons, houses, papers, and effects against unreasonable seizures and searches may not be violated” (Cal. Const., art. I, § 13.)
In *People v. Blair*, *supra*, 25 Cal.3d 640, the court rejected the rationale of *Smith v. Maryland*, *supra*, 442 U.S. 735, and concluded that telephone records, like the bank records found protected under California law in *Burrows v. Superior Court*, *supra*, 13 Cal.3d 238, were protected against unreasonable searches and seizures in California. (*Id.* at p. 653.) In *Blair*, the telephone records were obtained by a subpoena issued by a Federal Bureau of Investigation agent under authority of a United States Attorney as authorized by a federal grand jury. The court found that the federal subpoena was insufficient for purposes of the search and seizure provisions of the California Constitution since there had been no prior “judicial determination that law enforcement officials were entitled” to the records. (*Id.* at p. 655; see *Carlson v. Superior Court* (1976) 58 Cal.App.3d 13, 21-23.) Consequently, the seizure of the telephone records was ruled a violation of article I, section 13 of the California Constitution.

We believe that telephone calling records would additionally be protected under article I, section 1 of the California Constitution, which provides:

“All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.”

Under the rationale of *Burrows* and *Blair*, information obtained from pen registers and trap and trace devices would fall within the zone of privacy protected by the state Constitution, since the records of incoming or outgoing calls could lead to the discovery of an individual’s “virtual current biography” (*People v. Blair*, *supra*, 25 Cal.3d at p. 653, *Burrows v. Superior Court*, *supra*, 13 Cal.3d at p. 247; *People v. Chapman*, *supra*, 36 Cal.3d at p. 109.)

Based upon the foregoing, we find that the California Constitution allows the placement of pen registers and trap and trace devices only if a judicial ruling is first obtained that the law enforcement officers are entitled to the records. (*See 69 Ops.Cal.Atty.Gen., *supra*, at p. 59.) Do the court procedures set forth in federal law meet this state constitutional standard for prior judicial review? They do not.

The federal statutory scheme permits state law enforcement officers to apply for a state court order authorizing the use of a pen register or trap and trace device based upon a written certification that the information is “relevant to an ongoing criminal investigation.” (18 U.S.C. § 3122(b)(2).) Upon a proper application, the court must issue the order. (18 U.S.C. § 3122(a)(2).) The statutes do not authorize a court to go outside the written certification (*In re Order Authorizing Installation of Pen Reg.* (M.D.Fla. 1994) 846...
F.Supp. 1555, 1559), thus making the judicial review “ministerial in nature” (United States v. Fregoso (8th Cir. 1995) 60 F.3d 1314, 1320).

Under Burrows and Blair, this federal statutory process is inadequate to protect a California resident’s privacy interests in telephone calling records. As previously noted, the federal subpoena in Blair was found not to constitute appropriate “legal process” because issuance of the subpoena was a ministerial act with no “judicial determination” that the issuer was “entitled” to obtain the information. (People v. Blair, supra, 25 Cal.3d at pp. 651, 655.) A seizure of information is unreasonable when “the character, scope, and relevancy of the material obtained were determined entirely by the exercise of the unbridled discretion of the police.” (People v Chapman, supra, 36 Cal.3d at p. 113, quoting Burrows v. Superior Court, supra, 13 Cal.3d at p. 243; see People v. Blair, supra, 25 Cal.3d at p. 651.)

The federal statutes governing pen registers and trap and trace devices likewise fail the California constitutional test. No adequate prior judicial review is provided in the statutory scheme; rather, unbridled discretion is given to law enforcement officers.

We conclude in answer to the first question that the federal statutes governing the installation of pen registers and trap and trace devices do not provide authority for issuance of a state court order permitting a state law enforcement officer to install or use pen registers or trap and trace devices.

2. State Administrative Subpoena Statutes

Government Code section 11180\(^7\) authorizes the head of each of the state’s departments to conduct investigations concerning matters relating to the subjects under the department’s jurisdiction. Included within this power is the right to subpoena records. (§ 11181, subd. (e).) The department head may delegate subpoena powers to any officer of the department authorized to conduct the investigation. (§ 11182.)

Significantly, the department head or designee may issue a subpoena for investigative purposes in the absence of any formal charge or court proceeding. (§§ 11180, 11181, Brovelli v Superior Court (1961) 56 Cal.2d 524, 527-528.) The subpoenas are returnable directly to the department head, and no provision is made for notice to a third party—such as a telephone customer— or for the filing of a motion to quash or other formal opposition. (Compare §§ 11181, 11184, 11187 with Pen. Code, §§

\(^7\) All references hereafter to the Government Code are by section number only
Instead, if the subpoenaed party fails to comply with the subpoena, the department head may apply to a court for an order enforcing the subpoena. (§ 11187.) If it appears at the hearing "that the subpoena was regularly issued . . . the court shall enter an order" enforcing the subpoena. (§ 11188, italics added.) Hence, judicial enforcement of administrative subpoenas is subject to a standard less exacting than that required for a criminal search warrant. (See Craib v Bulmash (1989) 49 Cal.3d 475, 481-486.)

Of course, "department heads cannot compel the production of evidence in disregard of . . . the constitutional provisions prohibiting unreasonable searches and seizures." (Brovelli v. Superior Court, supra, 56 Cal.2d at p. 529; see also Pacific-Union Club v. Superior Court (1991) 232 Cal.App.3d 60, 70, 79-80; Wood v. Superior Court (1985) 166 Cal.App.3d 1138, 1146-1147) "[A] governmental administrative agency is not in a special or privileged category, exempt from the right of privacy requirements which must be met and honored generally by law enforcement officials." (Board of Medical Quality Assurance v. Gherardini (1979) 93 Cal.App.3d 669, 679-680; see Carlson v. Superior Court, supra, 58 Cal.App.3d at p. 22 ["Surely an accused’s constitutional right to privacy in his papers and records is not diminished because law enforcement officials seek to obtain them by subpoena rather than by warrant"]).

As with the federal statutes governing the installation of pen registers and trap and trace devices, the state administrative subpoena statutes do not contain a provision allowing for prior judicial review establishing that the law enforcement officers are entitled to the records. The California Constitution requires such prior review.

We conclude in answer to the second question that the state statutes governing the issuance of administrative subpoenas do not provide authority for a state law enforcement officer to install or use pen registers or trap and trace devices.

*****
THE PEOPLE, Plaintiff and Respondent, v. CRAIG BOYD DRENNAN, Defendant and Appellant.

No. C033959.

COURT OF APPEAL OF CALIFORNIA, THIRD APPELLATE DISTRICT


November 27, 2000, Decided


DISPOSITION: The judgment is reversed.

LexisNexis(R) Headnotes

COUNSEL: Dennis P. Riordan; Donald M. Horgan; and Dylan L. Schaffer for Defendant and Appellant.

Bill Lockyer, Attorney General, David P. Druliner, Chief Assistant Attorney General, Robert R. Anderson, Assistant Attorney General, Stephen G. Herndon and David Andrew Eldridge, Deputy Attorneys General, for Plaintiff and Respondent.

JUDGES: Opinion by Blease, Acting P. J., with Davis and Hull, JJ., concurring.

OPINIONBY: BLEASE

OPINION: [*1351] [**585]

BLEASE, Acting P. J.

Crag Boyd Drennan, who was superintendent of the Modoc Unified School District, was convicted of violating Penal Code section 632, subdivision (a) (intentional eavesdropping upon or recording of a confidential communication), based upon the installation of a hidden video camera, which took periodic photographs, without accompanying sound, of the area of the desk, computer, file cabinet, credenza and bookcase in the office of the Modoc High School principal. n1

---

n1 References to a section are to the Penal Code.

[***2]

We will reverse the judgment of conviction because the photographing of the principal's office for a purpose and in a manner which did not reveal the content of any conversation, was not an intentional act of recording a "confidential communication" as those terms are used in section 632.

FACTUAL AND PROCEDURAL BACKGROUND

Drennan is the superintendent of the Modoc Unified School District. n2 Dewey Pasquini was the principal at Modoc High School during the 1998-1999 school year.

n2 Drennan was on administrative leave at the time of trial.

Sometime prior to December 1998, Drennan asked the school district's attorney if it would be lawful to install a hidden camera in Pasquini's office to determine if someone was breaking into Pasquini's office and taking or reading confidential documents. The attorney informed him he lawfully could install the camera as long as it had no sound recording capabilities. Drennan also contacted the school board president and notified him of the camera. Drennan did not tell [***3] Pasquini about the camera.
Drennan directed James Lloyd, the maintenance supervisor for the school district, to hire someone to install the camera. The camera was installed in November 1998. After the camera was set up, Drennan viewed a tape of the area photographed. Drennan was not happy with the camera angle, because it showed the entire office. He was only interested in photographing the desk, file cabinets, bookcase, and credenza. The camera was moved two more times before Drennan was satisfied. [*1352]

The camera, hidden in a fake smoke detector, began operating in December 1998. It had no audio capabilities and was positioned to take pictures of Pasquini's desk, computer, file cabinet, bookcase and credenza. The camera was moved two more times before Drennan was satisfied. [*1352]

The camera, hidden in a fake smoke detector, began operating in December 1998. It had no audio capabilities and was positioned to take pictures of Pasquini's desk, computer, file cabinet, bookcase and credenza. The camera was moved two more times before Drennan was satisfied. [*1352]

The camera, hidden in a fake smoke detector, began operating in December 1998. It had no audio capabilities and was positioned to take pictures of Pasquini's desk, computer, file cabinet, bookcase and credenza. The camera was moved two more times before Drennan was satisfied. [*1352]

The camera, hidden in a fake smoke detector, began operating in December 1998. It had no audio capabilities and was positioned to take pictures of Pasquini's desk, computer, file cabinet, bookcase and credenza. The camera was moved two more times before Drennan was satisfied. [*1352]

The camera, hidden in a fake smoke detector, began operating in December 1998. It had no audio capabilities and was positioned to take pictures of Pasquini's desk, computer, file cabinet, bookcase and credenza. The camera was moved two more times before Drennan was satisfied. [*1352]

n3 We refer to the videotaping as taking pictures, because the camera, which took one frame every three seconds, did no more than take a series of still photos. It is doubtful whether the content of a communication could have been deciphered from such videotaping by (say) lip reading, had there been evidence that such was intended and accomplished. We have no occasion to determine whether such a means of accessing a communication is within section 632.

[***4]

Lloyd testified he ran out of tapes on a couple of occasions when Drennan had not: [*586] returned the tapes to him. On those occasions the camera was not operating. There were also times when the camera was not working because Lloyd was too busy to change the tapes. Drennan testified that he reviewed the tapes, but never saw "any two-party communication at any time while watching any of [the] tapes." Nor was his intention to watch what Mr. Pasquini was doing. Lloyd testified he recalled seeing one of the videotapes, but did not recall seeing anyone in the picture. However, he told a defense investigator he remembered seeing people coming in the room, but only recognized Pasquini.

Drennan directed Lloyd to stop taping in mid-March. The tapes had uncovered no evidence of a break-in of the office. Drennan instructed Lloyd to destroy the tapes and none of them survived to be admitted in evidence.

Pasquini testified that various agencies such as the sheriff's and police department used his office to conduct interviews. Teachers often had discussions with parents in the office as well. Usually, the door would be closed during these discussions. Pasquini felt the conversations [***5] which took place in his office were confidential in nature. One student testified he carried on several confidential conversations with Pasquini between November 1998 and March 15, 1999.

A jury found Drennan guilty of violating section 632, subdivision (a). The court sentenced Drennan to three years' felony probation on condition he serve 10 days in the county jail and pay fines and restitution in the sum of $ 7,010. The court stayed the jail time pending this appeal. [*1353]

DISCUSSION

(1a) At issue is whether the prohibition on eavesdropping upon a confidential communication, contained in section 632, subdivision (a), extends to the taking of timed still photographs, without accompanying sound.

We conclude it does not, nor does section 632 protect a general right of privacy from unconsented videotaping. Such a right enforced by penal sanctions is to be found in another section of the section 647, subdivision (k).

The trial court instructed the jury that "[c]ommunication . . . is not limited to conversations or oral communications, but rather encompasses any communication regardless of its form, including, but not limited to actions and signs where any party to the communication [***6] desires it to be confined thereto."

No evidence was presented that the videotaped photographs captured an image of persons communicating to anyone by means of actions or signs, the content of which could be deciphered. There was evidence that between November 1998 and March 1999, Pasquini's office was used to conduct confidential conversations. Although there is no direct evidence that such conduct was in fact photographed, it is inferred that it did occur in the manner permitted by the method and extent of the videotaping. Consistent with this inference, the People contend that section 632 prohibits the mere taking of the pictures of persons engaged in a confidential communication, and the term "recording" need not include the content of the communication. n4

n4 At trial, the prosecutor went further, telling the jury section 632 prohibited the video recording of mere conduct carried on in private. When defense counsel asked Pasquini whether the camera
recorded any confidential communication Pasquini had with another person, the prosecutor interposed a speaking objection: "That is misstates the law. It doesn't have to [be] a confidential communication with anybody else. It can be conduct by oneself."

In closing argument the prosecutor stated: "There's no requirement that anybody other than Mr. Pasquini be videotaped under that statute. Mr. Pasquini is in there and I asked him: Mr. Pasquini, is this your office? And he assumes that the door is closed and he assumes that what he's doing is private. He's got a right to do that. If he needs to pick his nose, he can pick his nose and nobody will record it. If he needs to scratch himself, same thing. Whatever. He's got a right to privacy in his own office."

The prosecutor's interpretation was clearly wrong. Section 632 prohibits the recording of a communication carried on "among the parties."

This requires the recording be of a communication between parties, not merely of the conduct of one or more persons.

[***7]

[**587] The People rely on People v. Gibbons (1989) 213 Cal. App. 3d 1204 [263 Cal. Rptr 905], from which their theory was apparently derived. Gibbons [*1354] held that a defendant who secretly videotaped his acts of sexual intercourse with various women violated the statute. Gibbons reasoned it "cannot be readily disputed" that "sexual relations is a form of communication, be it communication of love, simple affection, or, simply of oneself. " (Id. at p. 1209.) It acknowledged that "certain terms used in the privacy act, such as 'eavesdropping,' 'amplifying device' and 'telephone,' might suggest a narrow definition of communication, synonymous with conversation. However, the court said Penal Code section 630 expressly states the intent of the Legislature to protect the right of privacy of the people of this state. Consistent with the express declaration of intent and in the absence of any express statutory limitations, we find that 'communication' as used in the privacy act is not limited to conversations or oral communications but rather encompasses any communication, regardless of its form, where [*8] any party to the communication desires it to be confined to the parties thereto." (Ibid.)

We disagree both with this manner of statutory construction and with the conclusion reached.

(2) In interpreting a statute, the touchstone of meaning is the language used by the Legislature. (Zabetian v. Medical Board of California (2000) 80 Cal. App. 4th 462, 466 [94 Cal. Rptr 2d 917].) If the language is clear and unambiguous, we need not engage in judicial construction. Whether that is the case can be determined only when the language is sought to be applied to the case at hand. Each party will normally advance a candidate meaning of consequence to the party's position. If it cannot be determined from the language of the statute which is the correct application, extrinsic aids may be employed bearing on the objects to be achieved, the evils to be remedied, and the legislative history of the enactment. [Citation.] We call this an inquiry into legislative intent, i.e., an inquiry into the plausible meanings to be ascribed to the language in view of the history and context of [***9] the legislation. It does not sanction a judicial construction predicated upon a perceived policy which is not within the semantic constraints of the statutory language. The Legislature may make no law except by statute. (Cal. Const., art. IV, § 8, subd. (b))." (Id. at pp. 466-467, fn. omitted.)

(1b) In this case the language of both sections 630 and 632 rules out the construction placed upon the term "communication" by the Gibbons court. Section 632, subdivision (a), states in relevant part: "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 in the presence of one another or by means of a telegraph, telephone or other device, except a radio, shall be [***5] punished by a fine not exceeding two thousand five hundred dollars ($2,500) or imprisonment in the county jail not exceeding one year, or in the state prison, or by both that [***10] fine and imprisonment." n5

n5 The full text of section 632 is as follows: *(a) 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 in the presence of one another or by means of a telegraph, telephone or other device, except a radio, shall be [***5] punished by a fine not exceeding two thousand five hundred dollars ($2,500), or imprisonment in the county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment. If the person has previously been convicted of a violation of this section or Section 631, 632.5, 632.6, 632.7, or 636, the person shall be punished by a fine not
The statute is replete with words indicating the Legislature's intent to protect only sound-based or symbol-based communications. (3) The rule of statutory construction, noscitur a sociis, a word takes meaning from the company it keeps, is useful here. "A word of uncertain meaning may be known from its associates and its meaning 'enlarged or restrained by reference to the object of the whole clause in which it is used.' [Citation.""] (Oden v. Board of Administration (1994) 23 Cal. App. 4th 194, 203 [28 Cal. Rptr. 2d 388].)

Section 632 contains other words indicating the communications the Legislature seeks to protect are confidential [***12] communications conducted by sound or symbol. Subdivision (b) excludes from the ambit of the statute anyone known by all parties to the communication to be "overhearing or recording the communication." (Italics added.) Subdivision (c) excludes from the statute a communication the parties reasonably expect may be "overheard or recorded." (Italics added.) Subdivision (d) excludes evidence obtained as a result of "eavesdropping upon or recording a confidential communication" in violation of the section. (Italics added.) Subdivision (e) exempts from the statute certain "telephonic communication" systems. (Italics added.) Subdivision (f) exempts "hearing aids and similar devices, by persons afflicted with impaired hearing, for the purpose of overcoming the impairment to permit the hearing of sounds ordinarily audible to the human ear." (Italics added.)

Throughout section 632, subdivision (a), the juxtaposition of the words "eavesdrops" [***589] and "records" shows that when the Legislature used the word "records" it intended to prohibit two kinds of intrusion [***13] upon a communication: (1) a "real time" interception of a communication, by which the perpetrator listens to the communication as it occurs; and (2) a mechanical recording of a communication for later playback. The use of the word "records" was not intended as an independent basis upon which to make unlawful the photographing of conduct whether or not incident to a communication.

The language of the statute admits of no other construction than that the Legislature intended to address the interception and recording of sound-based or symbol-based communications, and that the statute protects the content of the communication from being recorded, not the non-contentbased conduct coincident to the communication.

That also can be gleaned from the Legislature's written expression of its intent contained in section 630. "The Legislature hereby declares that advances in
science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties [*14] and cannot be tolerated in a free and civilized society." (Italics added.) [*1357]

"Eavesdropping" is notably a term that refers to the surreptitious overhearing of conversations. That is made clear in the exception which section 630 recognizes, "that law enforcement agencies have a legitimate need to employ modern listening devices and techniques in the investigation of criminal conduct." It is manifest that it is listening in or eavesdropping upon private communications that the law seeks to remedy, not the taking of pictures of people engaged in conversation or other private conduct. It is in that context that section 630 declares the policy of the statute to "protect the right of privacy of the people of this state." This policy, contrary to the reasoning in Gibbons, is not a source of law independent of the elements of the statutory offense spelled out in section 632. Rather, section 630 makes clear that it is "the invasion of privacy resulting from the use of eavesdropping devices and techniques that section 632 seeks to remedy. (Italics added.)

We conclude from the repeated use of words associated with sounds, symbols and hearing that the recordings [*15] prohibited by this statute are the recordings of the contents of audible or symbol-based communications.

The legislative history of the statute supports this conclusion. On July 28, 1967, the Legislature passed Assembly Bill No. 860. Assembly Bill No. 860 was codified in part at chapter 1.5 of the Penal Code, commencing with section 630. (Stats. 1967, ch. 1505, § 1, pp. 3584-3588.) The Digest of Assembly Bill No. 860 (As Amended, June 5, 1967) by then Assembly Speaker Jesse M. Unruh, stated that the bill would change existing law (§ 653j) by requiring all parties to a confidential communication to give their consent to having the communication listened to or recorded. "Under existing law, Penal Code Section 653j, confidential conversations may be eavesdropped upon or recorded if only one party to the conversation gives his consent." (Italics added.) This shows that "communication" was equated with "conversation." ( People v. Gibbons, supra, 213 Cal. App. 3d at p. 1210 (dis. opn. of Campbell, J.).) The relevant wording of former section 653j is identical to that of section 632, suggesting the meaning of "communication" was carried over [*16] to the new law. n6

n6 Section 553j, subdivision (a) provided: "Every person or his authorized agent not a party to the communication who, intentionally and without the consent of any party to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records a confidential communication, whether such communication is carried on among such parties in the presence of one another or by means of a telegraph, telephone or other device, except a radio, shall be punished by imprisonment in the county jail not exceeding one year, or by fine not exceeding one thousand dollars ($ 1,000), or by both such fine and imprisonment." (Stats. 1963, ch. 1886, § 1, p. 3871.)

The Statement for the Floor on Assembly Bill No. 860 (As Amended in Senate, June [*590] 16, 1967) Relating to Invasions of Privacy (Statement) states, [*1358] "the measure [Assembly Bill No. 860] employs the present [section 653j] legal definition of a 'confidential communication' in defining [*17] conversations which would require two-party consent under the bill." (Statement, p. 4, italics added.) Again, this shows the Legislature equated "communication" with "conversation."

The Statement also asserts the bill relates to "the use of wiretap and electronic eavesdropping devices . . ." indicating only communications which can be overheard are the subject of the bill. The Statement specifies that under prior law only one party need consent "to the listening in," whereas the new law would require the consent of all parties. (Statement, supra, at p. 2, italics added.) "Presently it is entirely legal for one who receives a call to be totally unaware that it is being listened to clandestinely by another party. Likewise, a party may converse in person with another party who is secretly recording the conversation—he may be seriously injured by that conversation, either personally or in his business affairs—and he has no recourse at law. Assembly Bill 860 would correct this defect." (Ibid., italics added.) This is further evidence that the Legislature primarily equated "communication" with conversation, and that section 632 was meant to address [*18] sound-based communications.

These documents confirm what the language of section 632 states, that the Legislature intended to prohibit the recording of oral or telegraphic communications between two or more persons, not the photographing of two or more people carrying on a conversation. Such a video recording does not capture the communication itself, only evidence that a
Overview of Federal Laws & Cases, Capabilities & Limitations, and Practical Applications of Location-Based Electronic Surveillance and Off-Air Intercept

Prepared for:
FBI CALEA Implementation Unit’s Law Enforcement Technical Forum

*Some views expressed herein may not be consistent with official policy or argument of the Department of Justice

*Non-attribution is appreciated
Statutory Authorities

Pen-Trap
- Chapter 206 (§§ 3121-3127) of Title 18
  - Title III of 1986 ECPA, as amended

SCA
- Chapter 121 (§§ 2701-2712) of Title 18
  - Title II of 1986 ECPA, as amended

Tracking Devices (Definition & Jurisdiction)
- 18 USC § 3117
  - Section 108 of 1986 ECPA

FRCrP 41 (Search, Seizure & Tracking)
- Revised Dec. 2006 to include Tracking Devices
Terminology

- "Where's the phone pinging?"
- "Can you ping the phone?"
- What's a "Ping:"
  - Round-trip IP message?
  - Ordinary course tower/cell activation?
  - Forced registration of tower and cell?
  - GPS?
  - Triangulation?
Prospective (Live Intercept)

- Currently, only chapters
  - 119 (wiretap)
    - and
  - 206 (pen-trap)

...of Title 18 explicitly authorize ongoing, live intercept of either communications content (wiretap) or transactional records (pen-trap).
  - Wiretap for 30 days with renewals
    - Limited to communications CONTENT
  - Pen-Trap for 60 days with renewals
    - Limited to digits, addressing, routing and signaling
      - NO content
  - FRCrP 41 authorizes trespass/tracking into places that enjoy REP
  - Tracking for 45 days plus subsequent renewals
    - Communications to/from a tracking device are not electronic communications and are excepted from all confines of electronic surveillance law. 18:2510(12)(C).
Chapter 119's evidentiary threshold was legislated to be higher than Constitutionally required:

"Probable Cause Plus"

- 4th A. Privacy Interest? → YES
    - Supported Nardone v. U.S., 302 U.S. 379 (1937)
      - Sec. 605 of Communications Act of 1934 prohibits disclosure of intercepted communications by federal agents at trial.
    - Reversed Olmstead v. U.S., 277 U.S. 438 (1928)
      - Entry onto property required for unlawful intercept
    - Reversed Goldman v. U.S., 316 U.S. 129 (1940)
      - Trespass required for unlawful intercept

- Congress legislated higher protections
  - Title III of 1968 OCCSSA
  - Exhaust Other Methods & High-Level DOJ Review
  - Criminal Penalty for Unlawful Wiretap

- Although argued by EFF and FPD, not in-play for "cell-tracking cases"
Chapter 206's evidentiary threshold is the lowest found anywhere in criminal law: "Certification of Relevance"

- 4th A. Privacy Interest? → **NO**
  - *Smith v. Maryland*, 442 U.S. 735 (1979)
  - (no privacy interest in information voluntarily turned over to third party)

- Protected *only* through legislation
  - *ECPA* of 1986, as amended
    - "Addressing, Routing & Signaling Information attendant a Wire or Electronic Communication"
      - Added by USA PATRIOT in 2001
      - Includes Cell Site Information?
        - As first/last point of introduction/departure into the wireless provider's infrastructure
        - "Copper wire" equivalent
**Stored & Transactional Records**

Chapter 121 (18 USC §§ 2701-2712), created by Title II of 1986 ECPA

- "Stored Communications Act" is a *misnomer*.
  - Nothing explicitly states it has *prospective* efficacy
    - DOJ has argued it does (discussed later)
    - Nothing in FRCrP41 does either

- The word "transactional" does not appear in its body
  - Case law says chapter or section titles are irrelevant

- Access to anything not covered by wiretap or pen-trap
  - Contains three different evidentiary burdens
  - If it's not prospective, how do we get any non-content future transactional records (e.g. cell site activations)?
    - FRCrP 41 or 28:1651(b)(All Writs Act)?
SCA Standards:

Probable Cause (PC)
- Content 180 days old or more recent. 18 USC § 2703(a).
  - Unless stored on remote computing service→RS. 18 USC § 2703(b).
- Anything Else. 18 USC § 2703(c)(1)
  - including, arguably, E911 and cell sites (irrespective of call activity)

Reasonable Suspicion (RS), when seeking anything else.
- “A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service.”
  - RS defined as “specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.” 18 USC § 2703(d).

Relevance (inferentially)
- Grand Jury, Trial and Administrative Subpoenas
  - Narrowly defined list of items (modified in 2001 by USA PATRIOT)
    - Does include content on remote computing service, but...
    - Does NOT include cell sites.
The Hybrid Order

- The first "Combo-Order"
  (DOJ renamed it the "Hybrid" Order)

- Everyone signed it

- Pen-Trap with 2703(d) authority to obtain both
  - historical and future call detail with cell activations;
  - subscribers identified by the historical; and, often
    - call detail records (w/o cells), as well;
    - Necessary to identify new phone from common calls when fugitive
      "tossed" the original target

- Industry accepted these orders
  - became the standard across the country.
MJ Smith, S.D. Tex (Houston), new to the bench, was second to write an opinion:

- First opinion by MJ Orenstein, E.D. N.Y. (Central Islip) was a factually inaccurate opinion. His denial on motion for reconsideration is much better and largely quotes Smith.

- Much of Smith's opinion includes quotes of factually misstatements contained in the US Attorneys Manual. Smith is cited by every other opinion denying the government's applications.

- In all, 36 Opinions by 24 judges (14 MJs, 9 DJs, 1 Circuit Panel) have issued. Eight of those judges have written 2-3 times each.
Smith found...

2703(d) has no future efficacy and was not intended by Congress to be used in conjunction with Pen-Trap to overcome the 47:1002 impediment to disclosing a subscriber's location.

Receipt of future cell activations constitutes the installation and use of a tracking device.

There is no statutory mechanism that authorizes disclosure of future cell sites. Thus, FRCrP 41 and probable cause are the default even if it's not a tracker.
...but Smith was reversed.
USDJ Rosenthal held:

Hybrid Theory okay using 2703(d) R/S standard:

- Government *may* obtain "cell-site information at the origin and termination of calls and, if reasonably available, during the progress of a call that is not initiated by the government itself."
- Government **MAY NOT**:
  - Obtain GPS Locations
  - Obtain Triangulation Calculations (from telecomm)
  - Repeatedly call target or otherwise track the phone through cell site activations when no call is in progress
- Evidentiary question for obtaining GPS and triangulation not addressed.
  - Implicitly, PC required; but NOT necessarily for 4th A reasons (lack of Congressionally endorsed mechanism).
What if we want GPS and Triangulation? What if the Courts Reject Hybrid Theory?

- Although GPS and triangulation continues to be available in some federal jurisdictions throughout the country with a mere R/S showing, our general practice is:
  - NOT TO OBTAIN these more accurate calculations, which do not exist in the ordinary course

- unless we have:
  - PC-based Court Order, or
  - Exigent Circumstances (life or death/kidnapping/cop killer)
Hybrid vs. Search Warrant for Cells Score:

- **3 DJ & 4 MJ** support Hybrid Theory
  - 2d Cir: E.D.N.Y. & S.D.N.Y. (2 DJ, 1 MJ)
  - 5th Cir: S.D. Tex. DJ And W.D. La MJ
  - 9th Cir: E.D. Cal. MJ

- **3 DJ & 9 MJ** reject Hybrid Theory
  - 1st Cir: D.P.R. (Secured (sic.) Communications Act)
  - 2nd Cir: W.D.N.Y. MJ
  - 3rd Cir: All W.D.Penn MJJs (historical cells)
  - 4th Cir: D. Md, D.DC,
  - 7th Cir: N.D. Ind., E.D. Wis.

- **3 DJ & 2 MJ & Circuit Panel**
  - 1st Cir: D.Mass DJ; PC not required for historical cells
  - 4th Cir. S.D.W. Va MJ: “user” not protected as “Subscriber”
  - 6th Cir: E.D. Tenn. DJ & MJ: denying cell/E911 suppression motion
  - 7th Cir: S.D. Ill. Circuit Panel & DJ: no suppression of OTA evidence
Handset-Based 911 Solutions

- GPS is available *only* from Sprint-Nextel

**iDEN (Nextel National Network)**
- AGPS - Assistance provides quick first fix (seconds)
- Cell Tower (lat/long of cell tower) used for back-up

**CDMA (Nationwide Sprint PCS Network)**
- AGPS - Assistance provides quick first fix (seconds)
- Hybrid - AGPS/AFLT
- AFLT - Advanced Forward Link Trilateration
- Cell Tower & Sector
Multiple technologies provide the best fix

AGPS Fix ... open sky
AGPS Fix requires a minimum of three GPS measurements. "Assisted" because network assists device in first fix. Fewer

Hybrid Fix ... partial view of sky
CDMA pilot phase measurements can be used as a virtual GPS measurement in fixing position. If no GPS measurements are possible, attempt AFLT fix.

AFLT Fix ... indoors
Advanced Forward Link Trilateration (AFLT) Fix requires a minimum of three CDMA pilot Phase measurements to fix position in accordance with TDOA (Time Difference of Arrival) theory. If less than three are available, use Cell/Sector.

Cell/Sector Fix ... indoors, edge coverage
Cell/Sector location reports the center of the cell/sector

© 2006 Sprint Nextel. All rights reserved.
$30/mo...Track to Your Heart's Content

Welcome Steven!

Create a Request

View a Request

Back to Case

Other Targets

432-212-1510

Select

NOTE: Precision location requests may not be covert and the mobile device may exhibit a specific behavior associated with GPS requests.

Unsuccessful precision locations are not billed. To modify your default sent to, click on the accounts tab and modify the precision location section.

Monthly Fee of $30.00.

Locate At An Interval [4322121510]

Use this if you want to locate the target on a reoccurring basis.

Locate Once [4322121510]

Use this to locate the target once.

Scheduled Job: Ping every [ ] minutes [ ] minutes

(24 Hour Time) From [ ] To [ ] EST

Remote Delivery Options

Optionally you can have the output sent to an email or text message address.

Target's Alias: [ ]

Email: [ ] Add

Phone: [ ] Add

Verify Email/Text

Delete: [ ] 713530473@vtext.com

Delete: [ ] Steve.Lowenstein@VZW.Blackberry.net
Network-Based E911 Solutions

Triangulation available from AT&T & T-Mobile

- **AT&T**
  - GSM 850/1900 (Cell/PCS)
  - UMTS 850/1900 (Cell/PCS)

- **T-Mobile**
  - GSM 1900 (PCS)
    - E911-capable tower triangulation
      - based on Actual Ordered Timing Advance
      - 550m increments
  - UMTS 1700/2100 (AWS)
E911 Triangulation at Work
Basis, Advantages & Limitations of an E911 Approach in Lieu of Cells

For these providers, we prefer a PC-based order because

- Cheaper
- Faster
- More precise than cells

Don't always need to install the pen-trap intercept

L-Site/WebMap easy for Providers to Configure

**Location often, but not always, more precise than cells**

**BIG DRAWBACK for E911:**

Don't know when phone is in use.

- 3931 -
Authority:

Pursuant to 18 U.S.C. §§ 3123(a)(1) and 3127(3) and 18 U.S.C. § 2703(c)(1)(A) & (d) and Fed. R. Crim. P. 41, the Court finds that Affiant has offered sufficient evidence, amounting to probable cause, to believe that a crime has been committed, that Subject committed that crime, is charged and has filed; and that the information likely to be received from the proposed disclosure of location-based services will assist law enforcement in apprehending Subject.

Therefore, the Investigative Agency is authorized to require Provider to disclose the results (through any means reasonably available) of any and all available location-based services, including but not limited to real-time cell-site data irrespective of call activity and those Enhanced-911 (“E911”) services developed by the Provider in order to comply with the provisions of 47 C.F.R. §20.18. It is further ordered, consistent with the provisions of 18 U.S.C. §§ 2703(e) and 3124(d), that no cause of action shall lie against Provider for complying with this Order.
Cell-Sites Alone May Be Sufficient

- Ranging calculations for historical calls are available from Verizon Wireless & Alltel Wireless
  - Does NOT require PC-based order
  - Records exist in ordinary course, whether or not law enforcement requests their preservation or collection.

- Radiological Location Methods:
  - Signal Strength Measurements
    - Signal Attenuation as Function of Distance
    - Weather, Terrain, Buildings
  - Angle of Arrival Measurements
    - Requires Several Simultaneous Tower Measurements
    - Multipath Problems
  - Time-Based Measurements
    - Time of Arrival (TOA)
      - Must know time of departure
    - Difference in Times of Arrival (TDOA)
      - Measured from two receivers simultaneously
Cell-Sites Alone May Be Sufficient

- Using Time of Arrival (TOA)
  - Motorola CDMA switches:
    - `ACCESS_PN_CHIP_OFFSET`
      - when multiplied by 122 (1/2 PN chip-rate), will return the distance from the tower in meters with an average margin of error of 42.8 meters and standard deviation of 31.4 meters.
      - 1/10 PN chip-rate → 13.7m mean and 11.5m SD

- `INIT_MAHO_CAND1_BTS` and `INIT_MAHO_CAND1_SECTOR`
  - identify the first, second and third manual handoff tower/sector candidates that the phone reports back to the tower.
  - Fields labeled 2 and 3 with the same names
Cell-Sites Alone May Be Sufficient

- These and all other CDMA providers other than Sprint...
  - have no known remotely-activated E911 location capability
  - Don’t know how to give ranging calculations
  - So…getting a PC-based order provides no additional benefit
SSgt Lawrence Sprader
3rd ID, Ft. Hood, Texas

- Called 1Sgt from Cell on LandNav Course in middle of July 2007: “I’m Lost”
- Never heard from again.
- 5,000 Soldiers, Cops, etc. searched S-Mon.
- LE EISur received call Mon morning at 9a
- Provided location at 11a.
- Found that afternoon – 35m from estimate and 300m from CP (area had been searched 3x)
The prohibition in 47:1002(a)(2)(B) precludes *only* the telecommunications provider from disclosing information that may identify the subscriber's location.

- Law enforcement may intercept addressing, routing and signaling information associated with a communication *itself*
  - Only a "naked" pen-trap order is required

- FBI's self-imposed restriction
  - Stop and get a warrant once it is apparent subject may be inside a residence
How about Emergencies?

- We require a federal or state agency to make a written emergency declaration, pursuant to 18 USC § 3125 or state code authority, before we will collect pen-trap data or use our equipment to off-air collect.

- The agent signing the paper is on the hook to apply for a court order w/in 48 hours...NOT the Fed EISur.

  - Feds: High-ranking DOJ CRM OEO approval.
    - Slow game of phone tag from duty-AUSA up to main Justice.

  - States: DA or designee declares emergency pursuant to an express state code authorization
    - Much faster...sometimes 15 minutes.
    - States must have their own emergency provision
      - Cannot rely on the federal emergency provision
      - Provider’s Terms of Service???
Designating Officers for Emergencies

- State MUST have its own emergency statutes
  - Cannot rely on federal emergency provisions
- DA should designate specially trained officers
  - Often similar to officers authorized to conduct emergency wiretap
  - Maintain list, conduct training
  - Define “Emergencies”

An identifiable and specific person (or class of persons, such as police officers) may die or be seriously injured if we wait for an order
  - Cop killers, armed escapees, kidnappers, crime sprees, bomb threats, etc.
  - Perhaps flight to another country?
Fugitive Disentitlement

The Supreme Court has "sustained the authority of an appellate court to dismiss an appeal or writ in a criminal matter when the party seeking relief becomes a fugitive."


Until such time as Subject submits to the jurisdiction of the Court, he should not be permitted to enjoy a one-way communication that notices him on the precise ways and means through which the court and its marshals are attempting to locate him.

Escapee has no REP in Home or Hotel
Questions?
offense of possession with intent to distribute. He argues that the second prong is satisfied because (1) a jury could rationally have acquitted him of possession with intent to distribute had it believed Finley's testimony that he did not know the purpose of the truck-stop trip and disbelieved Brown's testimony to the contrary and (2) a jury could also have rationally convicted him of simple possession of methamphetamine if, based on the methamphetamine found in the pill bottles, it had believed Brown's testimony that he gave Finley methamphetamine in the van and disbelieved Finley's testimony that none of the methamphetamine in the van belonged to him.

We need not address Finley's argument under the second prong because he mistakenly assumes under the first prong that simple possession of the methamphetamine in the pill bottle is a lesser included offense of possession with intent to distribute the methamphetamine in the cigarette package. It is not; they are two separate, independent offenses.

"One offense is necessarily included in another if it is impossible to commit the greater without also having committed the lesser." 3 Charles Alan Wright, Nancy J. King, & Susan R. Klein, Federal Practice and Procedure § 515 (3d ed. 2004). "This rule is an application of the familiar Blockburger elements test, which the [Supreme] Court has adopted to determine when offenses are the 'same' under the Double Jeopardy Clause." Id.; see also Rutledge v. United States, 517 U.S. 292, 297 (1996).
It is well established that, in the abstract, simple possession of a controlled substance under 21 U.S.C. § 844(a) is a lesser included offense of possession with intent to distribute under 21 U.S.C. § 841(a)(1). United States v. Lucien, 61 F.3d 366, 372-74 (5th Cir. 1995). But under the Blockburger rule, possession with intent to distribute and simple possession constitute only one offense only where "the same act or transaction constitutes a violation" of both § 841(a)(1) and § 844(a). Rutledge, 517 U.S. at 297 (emphasis added) (quoting Blockburger v. United States, 284 U.S. 299, 304 (1932)). If, however, the greater offense of possession with intent to distribute and the lesser offense of simple possession arise out of two separate acts, and not "the same act or transaction," then the lesser offense is not included in the greater. See Blockburger, 284 U.S. at 301-03 (holding that two unlawful sales of narcotics to the same purchaser on consecutive days constituted two offenses, punishable separately).

In United States v. Johnson, the defendant was convicted of one count of possession of amphetamine in violation of § 844(a) and a separate count of possession with intent to distribute amphetamine in violation of § 841(a)(1) and 18 U.S.C. § 2. 977 F.2d 1360, 1373 (10th Cir. 1992). The defendant argued that his multiple convictions for amphetamine possession violated the Double Jeopardy Clause because they arose out of a single course of conduct. Id. at 1371. But the court disagreed. The court
acknowledged that "as to a single cache of drugs, simple possession under § 844(a) is a lesser included offense of possession with intent to distribute under § 841(a)(1)." Id. at 1373 (emphasis added) (citing Brown v. Ohio, 432 U.S. 161, 169 (1977); United States v. Burns, 624 F.2d 95 (10th Cir. 1980)). But it reasoned that the situation in that case differed because the amphetamine was found in two separate stashes and each stash was intended for a different purpose or transaction; one stash was intended for personal use and the other for distribution. See id. at 1373-74. Each stash therefore constituted a different criminal transaction. Id. at 1374.

We agree with Johnson's rationale. Applying it to the facts of this case, the methamphetamine in the cigarette package and the methamphetamine in the pill bottle were two separate caches of drugs; one was intended for distribution to Stratton at the truck stop, and the other was intended for some other purpose. Each stash therefore constituted a separate violation of the narcotics laws.

The government chose to prosecute Finley for the violation arising from the methamphetamine in the cigarette package only and not the methamphetamine in the pill bottle. The lesser

---

3 We recognize that the indictment's language was general; it did not specifically refer to the methamphetamine in the cigarette package and did not by its language exclude the drugs in the pill bottle.

But the government's theory of the case was that, by driving
included offense of possession with intent to distribute the methamphetamine in the cigarette package would be simple possession of the same stash of methamphetamine. But Finley’s

Finley to the truck stop knowing that the purpose was for methamphetamine distribution, Finley aided and abetted Brown’s possession with intent to distribute the methamphetamine in the cigarette package. And the arguments presented at trial made it clear to both the jury and the judge that Finley was on trial for the methamphetamine sold to Stratton and not for the methamphetamine in the pill bottle.

For example, in his closing argument, Finley’s counsel told the jury:

They’ve got to prove to you that Jacob [Finley] in his mind knew what was going on when Mark Brown delivered [the methamphetamine].

.......

It’s not what is in the orange bottle. There is no evidence of any intent to distribute that. It’s what was given—sold to Amy Stratton.

.......

Now, we know [Finley] is only accused of this one delivery to Amy Stratton.

There is no evidence that the methamphetamine in that orange prescription bottle, the orange cap, involved intent to distribute at all. There is no evidence of that. Nor on the residue, the little tiny traces, in the one with the white cap.

Counsel for the government did discuss the pill bottles found in Finley’s van, but she did so only to demonstrate Finley’s knowledge of Brown’s methamphetamine dealing and to question Finley’s credibility. The government never asserted that the jury could convict Finley on the basis of the methamphetamine in the orange-capped pill bottle or that Finley intended to distribute this methamphetamine.
argument rests solely on the methamphetamine in the pill bottle; he does not contend, nor did he before the trial court, that he is entitled to a lesser-included-offense instruction on simple possession of the methamphetamine in the cigarette package. Even if he did, on the evidence presented at trial, a jury could not rationally have convicted Finley of simple possession of this cache of methamphetamine and yet have acquitted him of possession with intent to distribute it. This is because the only issue at trial was Finley's knowledge of Brown's plan—i.e., whether Finley drove Brown to the truck stop knowing of Brown's plan or did so completely unwittingly. If Finley knew beforehand that the purpose of the trip to the truck stop was to distribute

---

4 During her closing argument, counsel for the government framed the issue as follows:

The only question in this case is: Did the Defendant know what was going on on August 19th of 2005? That's the only question for you to decide because it is undisputed that he participated in the possession with intent to distribute on August 19th of 2005. The only question is his knowledge. That's what you are going to have to decide.

Likewise, in his opening statement, Finley's counsel presented the issue as follows:

\[\text{[W]}\text{hat is this case about? It's about what was in Jacob Finley's mind . . . .}

\[\text{. . . Did he know beyond a reasonable doubt that Mark Brown was about to deliver methamphetamine to Amy Stratton, this lady, this informant? Did he know a drug transaction was about to occur?}\]
methamphetamine, then he is criminally liable for the greater offense of possession with intent to distribute; if Finley did not know this, then he is liable for neither the greater offense of possession with intent to distribute nor the lesser offense of simple possession. The additional element required for a conviction on the greater offense—here, intent to distribute the methamphetamine in the cigarette package—was not in dispute, and Finley was therefore not entitled to an instruction on the lesser offense. See Sansone, 380 U.S. at 349.

III. WARRANTLESS SEARCH OF CELL PHONE

Finley next contends that the call records and text messages recovered during the search of his cell phone should have been suppressed.

A. Standing

The government suggests that Finley lacks standing to challenge the search of the cell phone. The government asserts that Finley did not have a reasonable expectation of privacy in the cell phone because it was a business phone issued to him by his uncle's business. We disagree.

In determining whether a defendant has a reasonable expectation of privacy sufficient to contest the validity of a search, we inquire "(1) whether the defendant is able to establish an actual, subjective expectation of privacy with respect to the place being searched or items being seized, and
whether that expectation of privacy is one which society would recognize as reasonable." United States v. Cardoza-Hinojosa, 140 F.3d 610, 614 (5th Cir. 1998) (quoting United States v. Kye Soo Lee, 898 F.2d 1034, 1037-38 (5th Cir. 1990)).

The factors we consider include

whether the defendant has a [property or] possessory interest in the thing seized or the place searched, whether he has a right to exclude others from that place, whether he has exhibited a subjective expectation of privacy that it would remain free from governmental intrusion, whether he took normal precautions to maintain privacy[,] and whether he was legitimately on the premises.

Id. at 615 (quoting United States v. Ibarra, 948 F.2d 903, 906 (5th Cir. 1991) (first alteration in original)).

The district court found that, although Finley’s employer issued him the cell phone, Finley nonetheless maintained a property interest in the phone, had a right to exclude others from using the phone, exhibited a subjective expectation of privacy in the phone, and took normal precautions to maintain his privacy in the phone. We review these findings for clear error. Id. at 613 (citing United States v. Kelley, 981 F.2d 1464, 1467 (5th Cir. 1993)). The district court also determined that Finley had standing to contest the search. We review this conclusion de novo. Id.

The government concedes that Finley had a possessory interest in the cell phone and that his use of the phone weighs in favor of his right to challenge the search. The sole basis
for the government's argument appears to be that Finley's employer, not Finley, had a property interest in the phone and that Finley should have expected the employer to read the messages on the phone after he returned it to the employer. But a property interest in the item searched is only one factor in the analysis, and lack thereof is not dispositive. See, e.g., Mancusi v. DeForte, 392 U.S. 364, 368 (1968) ("[C]apacity to claim the protection of the [Fourth] Amendment depends not upon a property right in the invaded place but upon whether the area was one in which there was a reasonable expectation of freedom from governmental intrusion."); see also Cardoza-Hinojosa, 140 F.3d at 615 ("[N]o one of [the Ibarra] factors is necessarily conclusive . . . .").

The district court did not clearly err in finding that Finley had a right to exclude others from using the phone. That Finley's employer could have read the text messages once he returned the phone does not imply that a person in Finley's position should not have reasonably expected to be free from intrusion from both the government and the general public. Further, the government stipulated that Finley's employer permitted him to use the phone for his own personal purposes. And we see no error in the district court's finding that Finley

5 Although the district court found that Finley had a property interest in the phone, it appears that Finley's interest was possessory only and that his employer had the property interest in the phone.
took normal precautions to maintain his privacy in the phone, despite the government's protestation that the phone was not password protected. In these circumstances, we conclude that Finley had a reasonable expectation of privacy in the call records and text messages on the cell phone and that he therefore has standing to challenge the search.

B. Search Incident to Lawful Arrest

Although Finley has standing to challenge the retrieval of the call records and text messages from his cell phone, we conclude that the search was lawful. It is well settled that "in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a 'reasonable' search under that Amendment." United States v. Robinson, 414 U.S. 218, 235 (1973). Police officers are not constrained to search only for weapons or instruments of escape on the arrestee's person; they may also, without any additional justification, look for evidence of the arrestee's crime on his person in order to preserve it for use at trial. See id. at 233-34. The permissible scope of a search incident to a lawful arrest extends to containers found on the arrestee's person. United States v. Johnson, 846 F.2d 279, 282 (5th Cir. 1988) (per curiam); see also New York v. Belton, 453 U.S. 454, 460-61 (1981) (holding that police may search containers, whether open or closed, located within arrestee's
reach); Robinson, 414 U.S. at 223-24 (upholding search of closed cigarette package on arrestee's person).

Finley concedes that the officers' post-arrest seizure of his cell phone from his pocket was lawful, but he argues that, since a cell phone is analogous to a closed container, the police had no authority to examine the phone's contents without a warrant. He relies on Walter v. United States, 447 U.S. 649 (1980), for this proposition. Walter, however, is inapposite because in that case no exception to the warrant requirement applied, see id. at 657, whereas here no warrant was required since the search was conducted pursuant to a valid custodial arrest, see Robinson, 414 U.S. at 235. Special Agent Cook was therefore permitted to search Finley's cell phone pursuant to his arrest. Cf. United States v. Ortiz, 84 F.3d 977, 984 (7th Cir.

6 Finley cites United States v. Chan, 830 F. Supp. 531, 534 (N.D. Cal. 1993) (analogizing numbers in pager's memory to contents of closed container). Although Finley relies on this case, the Chan court concluded that police officers may, incident to the defendant's arrest, retrieve numbers from the memory of a pager seized from the defendant's person. See id. at 535-36.

7 The fact that the search took place after the police transported Finley to Brown's residence does not alter our conclusion. Cf. United States v. Edwards, 415 U.S. 800, 803 (1974) ("[S]earches and seizures that could be made on the spot at the time of arrest may legally be conducted later when the accused arrives at the place of detention."). In general, as long as the administrative processes incident to the arrest and custody have not been completed, a search of effects seized from the defendant's person is still incident to the defendant's arrest. United States v. Ruigomez, 702 F.2d 61, 66 (5th Cir. 1983) (citing Edwards, 415 U.S. at 804). Although the police had moved Finley, the search was still substantially contemporaneous with his arrest and was therefore permissible.
1996) (upholding retrieval of information from pager as search incident to arrest). The district court correctly denied Finley’s motion to suppress the call records and text messages retrieved from his cell phone.

IV. FINLEY’S POST-ARREST INTERVIEW

A. Police Statements Challenging Finley’s Truthfulness

Finley contends that the district court abused its discretion by denying his request for a limiting instruction regarding a witness’s comment on his veracity.

1. Background

During the course of Finley’s post-arrest interview at Brown’s residence, Finley initially denied that he had ever

Likewise, United States v. Chadwick, 433 U.S. 1 (1977) is inapplicable. Chadwick held that,

[0]nce law enforcement officers have reduced luggage or other personal property not immediately associated with the person of the arrestee to their exclusive control, and there is no longer any danger that the arrestee might gain access to the property to seize a weapon or destroy evidence, a search of that property is no longer an incident of the arrest.

433 U.S. at 15 (emphasis added). Finley’s cell phone does not fit into the category of “property not immediately associated with [his] person” because it was on his person at the time of his arrest.

Although Finley initially advanced his arguments in a motion in limine, the district court treated the motion as a motion to suppress, and Finley orally moved to suppress the contents of the cell phone at the pretrial conference.
distributed methamphetamine. Special Agent Cook and Sergeant Russell confronted Finley with a text message on his phone that read, "Call Mark I need a 50." Finley told them that "50" referred to an ounce (fifty dollars' worth) of marijuana, not methamphetamine. Special Agent Cook and Sergeant Russell challenged Finley's assertion that an ounce of marijuana costs fifty dollars. The following exchange then occurred:

Sgt Russell: I'll tell you what, you better start telling the truth.
Finley: I'm telling the truth, sir.
Sgt Russell: No you[‘re] not.
SA Cook: No you[‘re] not telling us the truth.

A recording of the interview and a transcript of the recording were admitted at trial.

At the charge conference, Finley requested that the court instruct the jury to disregard Special Agent Cook's and Sergeant Russell's comments about Finley's veracity. The district court denied Finley's request, reasoning that the officers were simply trying to get the most accurate statement possible from their interview of Finley and that the statements were not being offered to bolster the evidence or to accuse Finley at trial.

2. Standard of Review

We review a properly preserved challenge to jury instructions for abuse of discretion. United States v. Daniels,
281 F.3d 168, 183 (5th Cir. 2002) (citing United States v. Huynh, 246 F.3d 734, 738 (5th Cir. 2001)). But when the issue was not properly raised before the district court, our review is for plain error. Id. (citing United States v. Caucci, 635 F.2d 441, 447 (5th Cir. Unit B Jan. 1981)).

At the time the recording and transcript were admitted into evidence, Finley did not object on the basis that the statements improperly permitted one witness to opine on the veracity of another. The government argues that our review is consequently for plain error only. But Finley did request later at the charge conference that the jury be instructed to disregard any comments about Finley's veracity. We need not resolve, however, whether Finley preserved his argument because, as we explain below, even under an abuse-of-discretion standard we discern no reversible error.

3. Analysis

Relying on United States v. Freitag, Finley maintains that a limiting instruction was necessary because the transcript of the interview involved a witness discussing the veracity of the accused. See 230 F.3d 1019, 1024 (7th Cir. 2000) ("Because credibility questions are for the jury, it is improper to ask one witness to comment on the veracity of the testimony of another witness." (citing United States v. Cole, 41 F.3d 303, 308 (7th Cir. 1994); United States v. Sullivan, 85 F.3d 743, 749-50 (1st

-21-

- 3958 -
Finley also relies on United States v. Dotson, 799 F.2d 189 (5th Cir. 1986), which discusses the propriety of offering opinion evidence to impeach the credibility of a witness at trial. But these cases are inapposite because the challenge to Finley's truthfulness occurred in a pretrial interview, not at trial during a witness's testimony. 9

The district court did not abuse its discretion by denying Finley's request to instruct the jury to disregard Special Agent Cook's and Sergeant Russell's remarks. Special Agent Cook and Sergeant Russell certainly accused Finley of being untruthful, but it was done in the context of police questioning, and the jury was permitted to hear the comments in their context. The jury would certainly have understood that the officers investigating Finley would not have believed him, and the jury would not have afforded those officers' remarks in the context of the interview any more weight than they would have afforded the fact that the government also disbelieved him and decided to prosecute him. Cf. Dubria v. Smith, 224 F.3d 995, 1001-02 & n.2 (9th Cir. 2000) (en banc) (concluding in habeas review that trial court did not err by refusing to redact portions of a tape and transcript wherein a detective, inter alia, made statements of disbelief of the defendant's story in the context of pretrial

9 Special Agent Cook testified at trial, but he did not opine on the witness stand that Finley was untruthful. Sergeant Russell did not testify.
police questioning because the questions and comments placed the defendant's answers in context, there was nothing in the detective's statements that suggested evidence or theories of the case that were not presented at trial, and the jury would give the statements "no more weight than they would the fact [the defendant] was charged by the prosecutor with murder or that the prosecutor clearly also disbelieved [the defendant])."

B. Rule 404(b) Evidence

1. Background

Finley finally contends that the district court erred by admitting evidence of his prior drug use and distribution. During Finley's interview with Special Agent Cook and Sergeant Russell, Finley admitted that he had used methamphetamine he received from Brown on two prior occasions: once in high school and once three days prior to his arrest. He also admitted to cocaine use once in high school. He admitted to getting his

10 Finley mischaracterizes Dubria's analysis. He asserts that the statements were permissible in that case only because the error was cured by the judge's limiting instructions. But the Dubria court did not rely on the limiting instructions as the basis for its holding. Instead, after concluding that there was no error, the court stated that "even if" it was error to admit the tapes and transcripts without redacting the detective's accusatory statements, any error was cured by the limiting instructions. 224 F.3d at 1002.

11 Finley was at least a year out of high school.
friends marijuana from Brown so many times that he "couldn't count," and he said that on one of those occasions, two to three weeks earlier, the bag from Brown that was supposed to contain entirely marijuana had some small shards of methamphetamine in the bottom. Finley objected to the inclusion of these statements in the recording and transcript of his interview. Additionally, Brown testified that during the approximately six months prior to his arrest, he had sold Finley methamphetamine five to ten times and that Finley had distributed some of this methamphetamine; Finley objected to this testimony as well. The district court overruled Finley's objections, concluding that the evidence was admissible under Rule 404(b) of the Federal Rules of Evidence, although the court did give the jury a limiting instruction prior to the recording of the interview being played for the jury and again in the jury charge.

2. Standard of Review

We review a district court's decision to admit Rule 404(b) evidence in a criminal case under a heightened abuse-of-discretion standard. United States v. Jackson, 339 F.3d 349, 354 (5th Cir. 2003) (citing United States v. Wisenbaker, 14 F.3d 1022, 1028 (5th Cir. 1994)). Even if the district court abused its discretion, reversal is not proper if the error was harmless. Id. (citing United States v. Torres, 114 F.3d 520, 526 (5th Cir. 1997)).
3. Analysis

Evidence of other crimes, wrongs, or acts is admissible "as proof of motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake or accident." FED. R. EVID. 404(b). We analyze the admissibility of evidence under Rule 404(b) in a two-step inquiry. "First, it must be determined that the extrinsic offense evidence is relevant to an issue other than the defendant's character. Second, the evidence must possess probative value that is not substantially outweighed by its undue prejudice and must meet the other requirements of Rule 403." United States v. Beechum, 582 F.2d 898, 911 (5th Cir. 1978) (en banc).

Evidence of Finley's past methamphetamine purchases from Brown and his past distributions of narcotics were relevant to show Finley's motive and intent. The central issue at trial was whether Finley intended to aid and abet Brown's methamphetamine distribution to Stratton by driving Brown to the truck stop. Finley's recent assistance in Brown's distribution of narcotics was relevant to show Finley's intent to assist him on the day of the sale at the truck stop. And evidence of Finley's recent use of methamphetamine he bought or received from Brown was relevant to show Finley's motive—i.e., he agreed to drive Brown to the truck stop in exchange for extra methamphetamine. Moreover, the district court did not err by concluding that any undue prejudice
did not substantially outweigh the evidence's probative value.

The district court may, however, have abused its discretion by admitting evidence of Finley's cocaine and methamphetamine use while he was in high school. Cf. United States v. McDonald, 905 F.2d 871, 875 (5th Cir. 1990) (concluding that evidence of defendant's past speed and cocaine use was not admissible to show defendant's knowledge that his car contained marijuana); United States v. Jimenez, 613 F.2d 1373, 1376 (5th Cir. 1980) (reviewing a conviction for heroin distribution and concluding that undue prejudice substantially outweighed probative value of evidence of cocaine possession one year later).

But we conclude on these facts that any error was harmless. There was more than sufficient proof of Finley's guilt absent this evidence, and any harm was minimized by the court's two admonishments to the jury to consider the evidence for very limited purposes only. See United States v. Taylor, 210 F.3d 311, 318 (5th Cir. 2000) ("[P]rejudicial effect [of Rule 404(b) evidence] may be minimized by a proper jury instruction.").

V. CONCLUSION

For the foregoing reasons, Finley's conviction is AFFIRMED.
### Retention Periods of Major Cellular Service Providers

Data gathered by the Computer Crime and Intellectual Property Section, U.S. Department of Justice

<table>
<thead>
<tr>
<th>Service</th>
<th>Verizon</th>
<th>T-Mobile</th>
<th>AT&amp;T/Cingular</th>
<th>Sprint</th>
<th>Nextel</th>
<th>Virgin Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subscriber Information</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Post-paid: 3-5 years*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pre-paid: 2 years</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call detail records</td>
<td>1 rolling year</td>
<td>Pre-paid: varies</td>
<td>Post-paid: 5-7 years</td>
<td>From mid-November 2007**</td>
<td>Unlimited</td>
<td>2 years</td>
</tr>
<tr>
<td>Cell towers used by phone</td>
<td>1 rolling year</td>
<td>6 months</td>
<td>60-90 days</td>
<td>From mid-November 2007</td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td><strong>Text message detail</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Post-paid: 5-7 years</td>
<td>1 rolling year</td>
<td>Pre-paid: 5-7 years</td>
<td>Post-paid: 5-7 years</td>
<td>From mid-November 2007**</td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td>Text message content</td>
<td>3-5 days</td>
<td></td>
<td></td>
<td>12 days</td>
<td></td>
<td>90 days (search warrant required)</td>
</tr>
<tr>
<td>Pictures</td>
<td>Only if on website (customer can add or delete pictures any time)</td>
<td>Can be stored online and are retained until deleted or service is canceled</td>
<td>--</td>
<td>Contact provider</td>
<td>Contact provider</td>
<td></td>
</tr>
<tr>
<td>IP session information</td>
<td>1 rolling year</td>
<td>72 hours (revolving IP addresses used for cell phones)</td>
<td>80 days</td>
<td>n/a</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>IP destination information</td>
<td>30 days</td>
<td></td>
<td>72 hours (revolving IP addresses used for cell phones)</td>
<td>60 days</td>
<td>n/a</td>
<td>--</td>
</tr>
<tr>
<td>Bill copies (post-paid only)</td>
<td>3-5 years, but only last 12 months readily available</td>
<td>5-7 years</td>
<td>7 years</td>
<td>7 years</td>
<td>n/a$^3$</td>
<td>--</td>
</tr>
<tr>
<td>Payment history (post-paid only)</td>
<td>3-5 years, check copies for 6 months*</td>
<td>5 years</td>
<td>Depends on length of service</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>n/a$^3$</td>
</tr>
<tr>
<td>Store Surveillance Videos</td>
<td>Typically 30 days</td>
<td>2 weeks</td>
<td>Depends. Most stores carry for 1-2 months</td>
<td>Depends</td>
<td>Depends</td>
<td>n/a</td>
</tr>
<tr>
<td>Service Applications</td>
<td>Post-paid: 3-5 years*</td>
<td>--</td>
<td>--</td>
<td>Depends</td>
<td>Depends</td>
<td>--</td>
</tr>
</tbody>
</table>

* May vary by former company
** For records older than mid-Nov. 2007, Sprint can only provide bill reprints with outgoing info
$^3$ No bill copies, but list of credit card transactions does not expire

August 2009

Law Enforcement Use Only

- 3964 -
1. Preservation of Evidence under 18 U.S.C. § 2703(f)

Agents may direct providers to preserve existing records pending the issuance of compulsory legal process. Such requests have no prospective effect, however.

In general, no law regulates how long network service providers must retain account records in the United States. Some providers retain records for months, others for hours, and others not at all. As a result, some evidence may be destroyed or lost before law enforcement can obtain the appropriate legal order compelling disclosure. For example, suppose that a crime occurs on Day 1, agents learn of the crime on Day 28, begin work on a search warrant on Day 29, and obtain the warrant on Day 32, only to learn that the network service provider deleted the records in the ordinary course of business on Day 30. To minimize the risk that evidence will be lost, the SCA permits the government to direct providers to "freeze" stored records and communications pursuant to 18 U.S.C. § 2703(f). Specifically, § 2703(f)(1) states:

A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

There is no legally prescribed format for § 2703(f) requests. While a simple phone call should be adequate, a fax or an email is safer practice because it both provides a paper record and guards against misunderstanding. Upon receipt of the government's request, the provider must retain the records for 90 days, renewable for another 90-day period upon a government request. See 18 U.S.C. § 2703(f)(2). A sample § 2703(f) letter appears in Appendix C.

Agents who send § 2703(f) letters to network service providers should be aware of two limitations. First, § 2703(f) letters should not be used prospectively to order providers to preserve records not yet created. If agents want providers to record information about future electronic communications, they should comply with the electronic surveillance statutes discussed in Chapter 4.

A second limitation of § 2703(f) is that some providers may be unable to comply effectively with § 2703(f) requests, or they may be unable to comply without taking actions that potentially could alert a suspect. In such a situation, the agent must weigh the benefit of preservation against the risk of alerting the subscriber. The key here is effective communication: agents should communicate with the network service provider before ordering the provider to take steps that may have unintended adverse effects. Investigators with questions about a provider's practices may also contact CCIPS at (202) 514-1026 for further assistance.
Imagine the police have an arrest warrant for a crime suspect, and they want to find the suspect to arrest him. They happen to know the suspect's cell phone number, so they want to go to the phone company and have the phone company tell the police the location of the suspect's phone. The phone company refuses to let the police get that information without a warrant, so the police go to a judge and apply for a search warrant based on the probable cause to believe that the location of the phone will help them execute the arrest warrant. Here's the interesting question: Should the judge sign the warrant application and issue the warrant? Or should the judge deny the warrant application?

On August 3, Magistrate Judge Susan K. Gauvey issued a fascinating opinion on this novel question: In the Matter of an Application of the United States of America for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone, 2011 U.S. Dist. Lexis 85638 (D. Md. 2011). Her answer: The Judge must deny the warrant application, as location information is broadly protected by the Fourth Amendment and government cannot use warrants to find out the location of people who have warrants out for their arrest. The timing of the case is extremely unusual, as it seems the case is moot and this is only an advisory opinion. If I understand the timing, Magistrate Judge Gauvey denied the application over a year ago, and the government was able to arrest the suspect some other way in the meantime. Judge Gauvey decided to hand down an opinion on the legal issue anyway, appointed defense counsel to argue for defense interests, and now, a year later, has handed down the opinion on why she denied that application back in 2010.

Still, the opinion is obviously intended to be important: It goes on for 172 pages in the slip opinion, or 60 pages single-spaced, and it reaches out to weigh in on a lot of big issues. I also note that her opinion includes excerpts from my recent House Judiciary Committee testimony (see pages 94–96 and 106 of the slip op). So I thought I would blog some thoughts on the opinion. I'll start with Judge Gauvey's opinion, then explain why I think it's wrong, and then turn to a few broader thoughts on the role of magistrate judges in surveillance law.

I. Judge Gauvey's Analysis

Here's the basic reasoning of the opinion. First Judge Gauvey creates what appears to be a new distinction in Fourth Amendment law: a distinction between (a) Fourth Amendment rights in location at a given time, and (b) Fourth Amendment rights in movement over time. According to Judge Gauvey, individuals have a reasonable expectation of privacy in both. There is a reasonable expectation of privacy as to a person's location if a person cannot be visually observed in that same way. And there is a reasonable expectation of privacy in movements, which Judge Gauvey seems to be taking from the DC Circuit's Maynard/Jones "mosaic theory" case (which the Supreme Court recently agreed to hear). Judge Gauvey then reasons that if everyone has this Fourth Amendment right, people who have warrants out for their arrest have this right to privacy, too. For that reason, the
information held by the phone company as to the location of the phone user is protected by the Fourth Amendment.

Judge Gauvey then considers whether the Fourth Amendment allows a warrant to be issued based on probable cause that the information will help execute an arrest warrant. She concludes the answer is no: A Fourth Amendment warrant requires probable cause that evidence or contraband is located in the place to be searched or that a person who committed a crime is in the place to be searched. Mere probable cause to believe that location information would help the police execute a warrant is not enough under the Fourth Amendment. Judge Gauvey speculates that the Supreme Court would probably allow such warrants if the issue reached the Supreme Court, but she concludes that she "will not take that leap in the absence of any direct precedent or sufficient doctrinal foundation, especially in the face of considerable legislative and public concern and discussion about the invasion of privacy that this new and evolving location technology permits." Judge Gauvey seems particularly unwilling to issue the warrant in light of all the hearings Congress has had over the past year on how the statutory surveillance law applies to cell-site location: "Against this backdrop of intense congressional inquiry and public concern," she writes, it is especially inappropriate to sanction an expansion of law enforcement acquisition of location data . . .

II. Why I Think Judge Gauvey's Decision is Wrong

My own view is that Judge Gauvey is pretty clearly wrong. Most fundamentally, I don't think location information of phones is protected by the Fourth Amendment under Smith v. Maryland, for all the reasons I have explained at length. Part of the problem is that the Fourth Amendment does not deal in abstractions, with categories such as the right to privacy in "location" or right to privacy in "movement." The Fourth Amendment is much more granular: The relevant question is whether the particular data stored in a particular place on a particular server is protected by the Fourth Amendment, and if so, who is it who has those rights and under what circumstances can that particular information be accessed and disclosed. Given that, Judge Gauvey's abstract categories produce more heat than light. It doesn't help that Judge Gauvey relies significantly on the "mosaic theory" opinion that the Supreme Court recently agreed to review.

Assuming Judge Gauvey is right that location information is in fact protected by the Fourth Amendment, then the next question is when the government can obtain a warrant to order the release of that information. This is actually a very interesting question of Fourth Amendment law. Notably, Payton v. New York concluded that "an arrest warrant founded on probable cause implicitly carries with it the limited authority to enter a dwelling in which the suspect lives when there is reason to believe the suspect is within," and it seems a it strange that the arrest warrant allows the police to break into a suspect's home but yet there is no ability to even get a warrant to find out the location of the suspect's phone. Judge Gauvey seems to think that it would require a novel extension of Payton to say that Payton allows a warrant for location information to find the suspect, but I think she has the novelty question a bit backwards: It's a novel application of the Fourth Amendment to say that it extends to location information, and that novelty sets up the new question of how Payton applies.

What's the answer? I think this part of the opinion is actually quite difficult, but I would tentatively think that Steagald v. United States is fairly read to allow a Fourth Amendment warrant in this situation. Steagald considered what the police must do when the police think a suspect is in someone else's home, and they want to execute an arrest warrant of the suspect there. Steagald ruled that the police must obtain a search warrant to do that: They must obtain a warrant to search the home for the
person inside to safeguard the Fourth Amendment interests of the people who live there. The basic idea is that the search warrant based on probable cause to think that the object of the arrest warrant will be there makes the search of the place reasonable. The Steagald court was not focused on whether the person in the house was "evidence of crime," but rather focused on the government's need to justify the intrusion. Although it's not an easy question, I think the same reasoning would justify a search of the phone company's computer for location information of the suspect's whereabouts to execute the warrant. But as I said, it's a tricky question — one set up by the novelty of concluding that location information is protected by the Fourth Amendment.

III. A Few Concluding Thoughts

I think this opinion is interesting in two main ways. First, it's yet another example of the recent practice of magistrate judges using their authority to grant or deny court order applications to hand down very broad opinions on novel issues of how the Fourth Amendment applies to computers and new technologies. I'm generally critical of this development, but it bodes well for those who strongly want the courts to be more civil libertarian in the surveillance law area. Because most judges will grant the applications without an opinion, but will be more interested in explaining why they denied an application, and because any judge can write an opinion at any time on why they are granting or denying the application, this procedure lets a few magistrate judges with very strong views (think Orenstein in New York or Smith in Texas) write opinions on novel questions when they rule on the application.

Although magistrate judges aren't Article III judges, the magistrates can still submit their opinions to the F.Supp.2d and get them published. As as we see in this case, they can order briefing and submit the opinion over a year after the case is moot. Over time, these magistrate judge opinions are having an impact on the law even though they arise from only a small handful of non-Article III judges in quite unusual procedural contexts. (On that note, I see that over at the Robing Room there is this lawyer's evaluation of Judge Gauvey form 2006: "She is extremely ambitious and fearless in using the publication of her rulings as a means to raise her profile.")

Second, this issue is worth keeping in mind for the pending Supreme Court litigation in United States v. Jones, the GPS/mosaic theory case. When the Fourth Amendment mostly protects only invading private spaces, the scope of the warrant authority is reasonably clear: The Fourth Amendment warrant can be obtained to invade the private space for evidence or the suspect. On the other hand, if the Fourth Amendment is read to extend to location information even in public places, then that extension begins to raise new questions of when a warrant can be obtained to access that location information where it has been generated. This is also worth noting for the statutory debate over location information in Congress: As I noted in the passage Judge Gauvey excerpts from my House testimony, probable cause of what is an essential question in applying the probable cause standard.