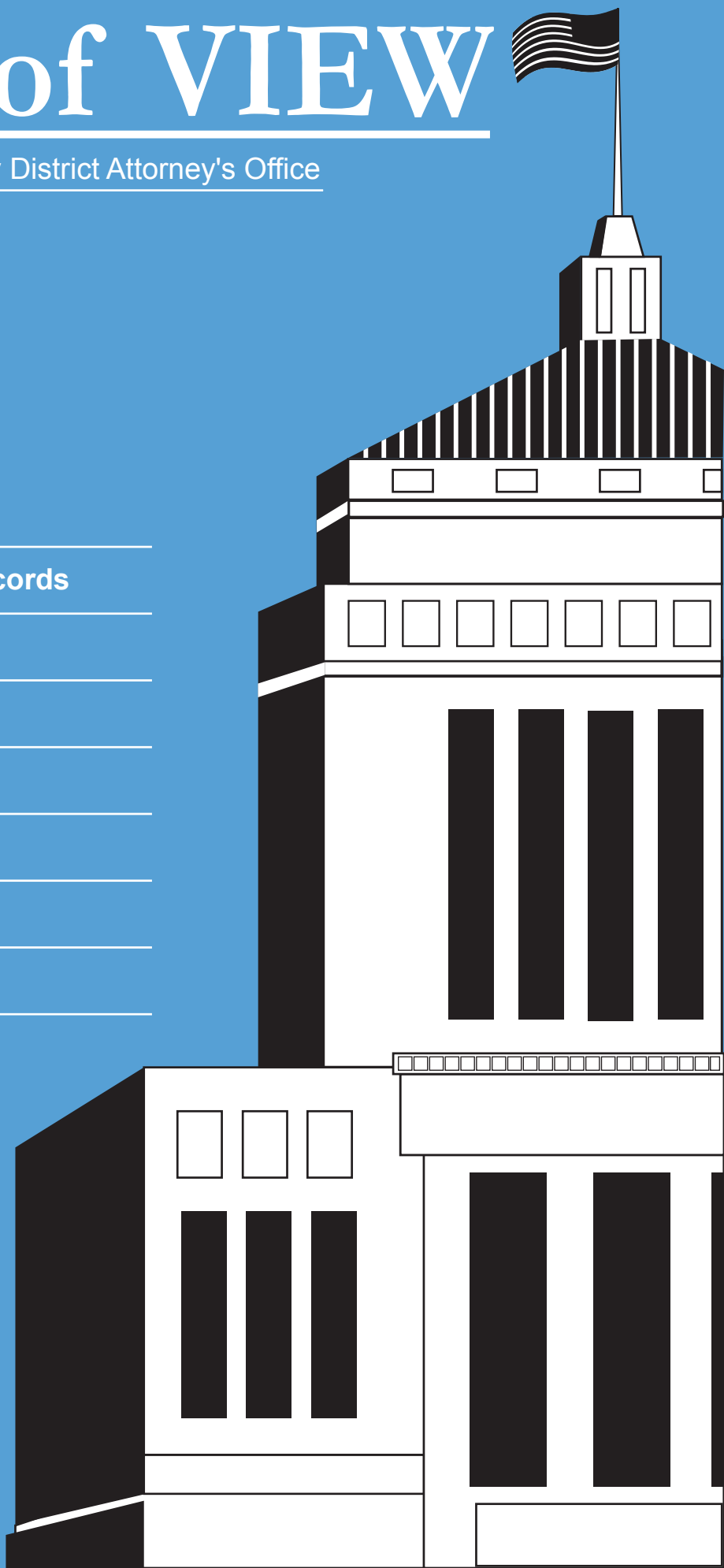
POINT of VIEW

A publication of the Alameda County District Attorney's Office

Nancy E. O'Malley, District Attorney

In this issue



WINTER 2012

Point of View

Since 1970

Executive Editor
Nancy E. O'Malley
District Attorney

Writer and Editor
Mark Hutchins

Point of View Online
Featuring new and archived articles and case reports
www.le.alcoda.org

• Volume 40 Number 1•

Point of View is published in January, April, July, and October. Articles and case reports may be reprinted by law enforcement and prosecuting agencies or for any educational purpose, if attributed to the Alameda County District Attorney's Office. Send correspondence to Point of View, District Attorney's Office, 1225 Fallon St., 9th Floor, Oakland, CA 94612. Email: POV@acgov.org.

This edition of Point of View
is dedicated to the memory of
Officer Jim Capoot
of the Vallejo Police Department
who was killed in the line of duty
on November 17, 2011

Contents

Electronic Communications

Obtaining Email, Voicemail, and Text Messages

SHAREE1013: Jerry I am scared.
Jlc1006: Me too—don't try to hide it.
SHAREE1013: Jerry, don't look at him, don't talk to him.
Jlc1006: Don't worry.
SHAREE1013: Just do it and get the hell out of there.

Emails from Sharee Miller and her boyfriend as they plot the murder of Miller's husband. *Miller* v. *Stovall* (2008) 573 F.Supp.2d 964.

Email, voicemail, and texting have changed the way almost everyone communicates these days, including co-conspirators. For example, a British Airways employee who had been recruited to help plant a bomb on an airliner received the following email from his recruiter, Anwar al Awlaki: "Our highest priority is the U.S. Anything there, even if on a smaller scale compared to what we may do in the U.K. would be our choice. So the question is: is it possible to get a package or a person with a package on board a flight heading to the U.S.?" (Anwar never got a satisfactory answer to his question; he was killed in a CIA-led drone strike.)

In another case, a man named Ron Williams was about to murder his wife in their home in Florida when he inadvertently hit the speed dial button on his cell phone which called the house. The call went to voicemail which captured the terrifying sounds of his wife being stabbed to death. Investigators obtained a copy of the voicemail, and prosecutors played it to the jury in Williams' murder trial. To no one's surprise, he was convicted.

As Ron Williams, Anwar al Awlaki, Sharee Miller and countless other felons have learned, electronic communications technology is as useful to criminal investigators as it is to the criminals themselves. But while the technology is helpful, the law that regulates it is not. In fact, courts and commentators have aptly described it as "dense and confusing,"[1] and "a complex, often convoluted area of the law."[2] As a result, officers, prosecutors, and even judges have often been unsure of the standards and procedures by which copies of these types of communications can be obtained from service providers.

Fortunately, the law in this area has developed to the point that it is now fairly intelligible. For this reason, we decided to revisit the subject and bring our readers up to date on how the courts have been deciding cases in which email, voicemail, and text messages were admitted as evidence in criminal trials. But to really grasp this subject, it is necessary to understand the framework upon which this area of the law has been built. So that is where we will start.

The Stored Communications Act

In the past, there were essentially only two ways for people to communicate if they were not within shouting distance: telephone and mail. Consequently, the rules were fairly simple: To intercept telephone conversations, officers needed a wiretap order; to read someone's mail, they needed a search warrant.[3]

In the 1980s, however, dramatic developments in computer and telecommunications technologies provided the public with much faster and more convenient ways to communicate, most notably email and voicemail, and later the cell phones and text messaging. As the Sixth Circuit observed last year:

> Email is the technological scion of tangible mail, and it plays an indispensable part in the Information Age. Over the last decade, email has become so pervasive that some persons may consider it to be an essential means or necessary instrument for self-expression, even self-identification.[4]

In a strange twist of fate, however, it turned out that the manner in which this new technology transmits messages rendered them "not private" under the Fourth Amendment. This was because the

[1] Orin S. Kerr, *A User's Guide to the Stored Communications Act*, (2004) 72 Geo. Wash. L. Rev. 1208.
[2] *U.S.* v. *Smith* (9th Cir. 1998) 155 F.3d 1051, 1055.
[3] See *Ex parte Jackson* (1877) 96 U.S. 727, 728 ["Whilst in the mail, [letters] can only be opened and examined under like warrant"].
[4] *U.S.* v. *Warshak* (6th Cir. 2011) 631 F.3d 266, 286 [quoting from *City of Ontario* v. *Quon* (2010) __ U.S. __ [130 S.Ct. 2619, 2631]].

Supreme Court has consistently ruled that, under the Fourth Amendment, a person cannot ordinarily expect privacy in information that he has transmitted through an intermediary.[5] And that is exactly what happens when a person sends an electronic communication because the message must be copied and stored along the way (at least temporarily) on equipment that is owned and controlled by the service provider. Thus, criminal investigators could (at least theoretically) obtain copies of electronic communications from providers by simply asking.

In reality, however, virtually everyone who communicates by email, voicemail, or texting expects that their messages will be private, especially since there is no reason for the providers or their employees to read them.[6] While it is almost certain that the Supreme Court will someday re-examine its rulings on the issue and address this discord, Congress acted first, having decided that if the Fourth Amendment did not protect the privacy of these forms of communications, it would write a law that did. The result was the Stored Communications Act of 1986 (SCA).[7]

As Congress was writing the SCA, one of the most important decisions it needed to make was whether the rules covering the acquisition of electronic communications by law enforcement would be subject to the same strict requirements that govern the interception of phone conversations and the reading of mail, or whether they should be subject to less restrictive standards. Ultimately, it decided to impose less restrictive standards, mainly because people who communicate in this manner know that their messages are stored and are easily copied and, thus, they have a somewhat reduced expectation that their messages will remain private.

While Congress made its intent on this issue clear, the bulk of the SCA was disorganized and poorly written. As Georgetown law professor Orin Kerr pointed out, judges, legislators, and even legal scholars "have had a very hard time making sense of the SCA."[8] To make matters worse, the courts have been unable or unwilling to clarify the various issues and provide the kinds of guidance that investigators desperately need. In fact, in 2010 when the United States Supreme Court had an opportunity to provide some direction, it not only ducked the issue, it advised the lower courts to do the same. Here are the Court's words: "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[9] And yet, the role of this technology will not become "clear" for decades (if not centuries) because it is constantly changing and expanding. As the Sixth Circuit warned in *United States* v. *Warshak*, "[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."[10]

So, given the failure of Congress to write a comprehensible explanation of the law and the Supreme Court's suggestion that the lower courts remain above the fray for a while, and also given the scarcity of published criminal cases in this area,[11] it is no wonder that officers, prosecutors, and judges might seem perplexed.

Nevertheless, as noted earlier, the fundamental principles and basic requirements of the law have become much more understandable lately, thanks mainly to a few judges and legal commentators who have attempted to penetrate this "dense and confusing" subject and make sense of it.

---

[5] See *Smith* v. *Maryland* (1979) 442 U.S. 735, 743; *United States* v. *Miller:* (1976) 425 U.S. 435, 443.

[6] **NOTE**: One indication that the Court may so rule is found in its decision in *City of Ontario* v. *Quon* (2010) __ U.S. __ [130 S.Ct. 2619]. In *Quon*, the Court could have simply resolved the issue by reaffirming its rule that people cannot reasonably expect privacy in stored text messages. Instead, it assumed for the sake of argument that stored text messages were, in fact, private under the Fourth Amendment. Also see *Wilson* v. *Moreau* (D.R.I. 2006) 440 F.Supp.2d 81, 108 ["the Court holds that Donald P. had a reasonable expectation of privacy in his personal Yahoo e-mail account"].

[7] 18 U.S.C. 2701 *et seq*.

[8] Orin S. Kerr, "A User's Guide to the Stored Communications Act," (2004) 72 Geo. Wash. L. Rev. 1208.

[9] *City of Ontario* v. *Quon* (2010) __ U.S. __ [130 S.Ct. 2619]. Also see *Rehberg* v. *Paulk* (11th Cir. 2010) 611 F.3d 828, 844 ["The Supreme Court's most-recent precedent *[Quon]* shows a marked lack of clarity in what privacy expectations as to content of electronic communications are reasonable."].

[10] (6th Cir. 2010) 631 F.3d 266, 285.

[11] **NOTE**: The lack of cases occurred because, as discussed below, the exclusionary rule does not apply to SCA violations; thus, there are no cases in which criminal defendants sought the suppression of evidence.

When the SCA applies

Theoretically, the first step in determining how to obtain copies of electronic communications is to figure out whether the communication falls within the protections of the SCA. In reality, however, it doesn't really matter because, even if the law does not apply (or even if the message was not "private" under the Fourth Amendment), officers will seldom be able to obtain any stored communication from a service provider unless they have legal authority for doing so. This is because providers risk being sued by their subscribers if they reveal communications without legal process. So they usually insist upon it.

In any event, a message falls within the SCA if (1) it was "stored," and (2) it was stored on the equipment of an "electronic communication service" (ECS) or a "remote computing service" (RCS).

WHAT'S A "STORED" COMMUNICATION? An electronic communication is deemed "stored" if it was being held temporarily by a provider as an incident to its transmission to the recipient. Thus, most courts have ruled that an email or other communication that has been opened by the recipient is no longer in temporary storage because it has reached its final destination.[12]

It should be noted, however, that the Ninth Circuit muddied things up when it announced its controversial decision in the case of *Theofel* v. *Farley-Jones.*[13] In *Theofel*, the court broadly defined the term "storage" to include the storage of all email held by a provider until it is "expired in the normal course" (whatever that means), even if it has been opened and is therefore no longer being stored incident to or pending delivery. Among the critics of this ruling was the preeminent authority on the subject who observed that "the Ninth Circuit's analysis in *Theofel* is quite implausible and hard to square with the statutory text."[14] In addition, the U.S. Department of Justice has written that "the Ninth Circuit's reasoning in *Theofel* confuses 'backup protection' with ordinary storage of a file."[15] But, for now, *Theofel* is still the law in this circuit.

ECSS AND RCSS: The SCA regulates the disclosure of electronic communications that are in the possession of an ECS or RCS available to the general public. Here, the term "electronic communication service" is broadly defined as "any service which provides to users thereof the ability to send wire or electronic communications,"[16] which would include internet, telephone, and email service providers.[17] In contrast, a website such as Amazon.com would not be deemed an ECS because it is in the business of processing sales orders which are not the type of communication that is covered under the SCA.[18]

As for "remote computing services," they are companies that provide "computer storage or pro-

[12] See *Steve Jackson Games, Inc.* v. *U.S. Secret Service* (5th Cir. 1994) 36 F.3d 457, 461; *DoubleClick Privacy Litigation* (S.D.N.Y. 2001) 154 F.Supp.2d 497, 511-12; *Fraser* v. *Nationwide Mutual Insurance Co.* (E.D. Pa. 2001) 135 F.Supp.2d 623, 635-36.

[13] (9th Cir. 2003) 359 F.3d 1066.

[14] Orin S. Kerr, *A User's Guide to the Stored Communications Act*, (2004) 72 Geo. Wash. L. Rev. 1217. Also see *U.S.* v. *Weaver* (C.D. Ill. 2009) 636 F.Supp.2d 769, 772 ["The Ninth Circuit's interpretation of storage for backup protection under the Stored Communication Act cannot be squared with legislative history and other provisions of the Act."].

[15] Computer Crime and Intellectual Property Section [of DOJ], "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" (Chapter 3 The Stored Communications Act), www.cybercrime, gov/ssmanual/03ssma.html, accessed September 2011.

[16] 18 U.S.C. § 2510(15).

[17] See *Quon* v. *Arch Wireless* (9th Cir. 2008) 529 F.3d 892, 903 [text messaging service was deemed an ECS] [overturned on other grounds in *City of Ontario* v. *Quon* (2010) __ U.S. __ [130 S.Ct. 2619]; *In re DoubleClick Inc. Privacy Litigation* (S.D.N.Y. 2001) 154 F.Supp.2d 497, 508 ["Access to the Internet is the service an ISP provides. Therefore, the 'service which provides to users thereof the ability to send or receive wire or electronic communications' is 'Internet access.'"]; *Freedman* v. *America Online* (E.D. Va. 2004) 325 F.Supp.2d 638, 643, fn.4 ["It is clear that AOL is a provider of 'electronic communication service'"].

[18] See *Crowley* v. *CyberSource Corp.* (N.D. Cal. 2001) 166 F.Supp.2d 1263, 1270 ["Crowley argues that Amazon is an electronic communication service provider because it receives electronic communications from customers, saying that 'without recipients such as Amazon.com, users would have no ability to send electronic information.' This argument was expressly rejected in *Andersen Consulting LLP* v. *UOP*, 991 F.Supp. 1041 (N.D.Ill.1998)."]; *In re Jetblue Airways Corp. Privacy Litigation* (E.D.N.Y. 2005) 379 F.Supp.2d 299, 307 ["Thus, a company such as JetBlue does not become an "electronic communication service" provider simply because it maintains a website that allows for the transmission of electronic communications between itself and its customers."]; *Dyer* v. *Northwest Airlines Corp.* (D.N.D. 2004) 334 F.Supp.2d 1196, 1199 ["Courts have concluded that 'electronic communication service' encompasses internet service providers as well as telecommunications companies whose lines carry internet traffic, but does not encompass businesses selling traditional products or services online."].

cessing services by means of an electronic communications system."[19] Thus, while most ECSs simply transmit and temporarily store information as an incident to the communication, RCSs store the information for other purposes, and may process it or otherwise make changes to it.[20]

It should be noted that the distinction between ECSs and RCSs is a holdover from 1980s technology and is no longer of much importance. That is because most people now utilize the services of internet service providers who are almost always ECSs or, at least, multifunctional.[21]

SEARCHING THE SUSPECT'S COMPUTER: It is important to understand that the procedures set forth in the SCA do not cover searches of email, voicemail, or text messages that have been stored on computers or other storage devices that are owned or controlled by the suspect. There are two reasons for this. First, the SCA covers only communications that have been stored with third-party providers. Second, even under *Theofel,* messages stored on a suspect's computer are not in temporary or intermediate storage because they do not "expire in the normal course."[22] But even though the SCA does not apply, the Fourth Amendment *does*, which means that officers will need a warrant to search a suspect's computer.

Communications vs. Records

Although the federal law is known as the Stored Communications Act, it also provides the means by which officers can obtain the *records* pertaining to those communications. This is significant because communication records often provide information that is just as important as the communications themselves. For example, investigators may be able to determine a suspect's whereabouts at a particular time by obtaining records that reveal the locations of cell phone towers that carried signals from his phone.

The SCA's role in obtaining records is also important because, while a search warrant is usually necessary to obtain communications, there are several other options when officers are seeking records. Because of this, and because communication records are so important to investigators, this subject is covered in a separate article starting on page 8.

The difference between communications and communications records is not, however, as clear cut as it might seem—especially when dealing with electronic communications. For this reason, it is necessary to briefly discuss these differences.

The term "electronic communications" (also called "content") refers to the message that is conveyed by the sender, including statements of fact, thoughts, requests, conclusions and other expressions. Thus, the federal wiretap law defines the term "contents" as including "any information concerning the substance, purport, or meaning of that communication."[23] Importantly, words may be deemed "communications" even if they are not technically a part of the message. For example, the subject line pertaining to an email message would likely be deemed "content."[24]

---

[19] 18 U.S.C. § 2711(2).

[20] **NOTES**: According to the U.S. Department of Justice, "Roughly speaking, a remote computing service is provided by an off-site computer that stores or processes data for a customer," such as a "service provider that allows customers to use its computing facilities" or a "server that allows users to store data for future retrieval." Computer Crime and Intellectual Property Section [of DOJ], "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" (Chapter 3 The Stored Communications Act), www.cybercrime, gov/ssmanual/03ssma.html, accessed September 2011.

[21] **NOTE**: For these reasons, a respected commentator in this area of the law has recommended that Congress eliminate "the confusing" ECS and RCS categories. Orin S. Kerr, *A User's Guide to the Stored Communications Act*, (2004) 72 Geo. Wash. L. Rev. 1209, 1215.

[22] See 18 U.S.C. 2510(17) ["electronic storage" means (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication *by an electronic communication service* for purposes of backup protection of such communication"; emphasis added].

[23] 18 U.S.C. § 2510(8). Also see 18 U.S.C. 2711(1); Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act*, 97 Nw U.L.Rev. 607, 611 ["[E]very communications network features two types of information: the contents of communications, and the addressing and routing information that the networks use to deliver the contents of communication."].

[24] See *In re Application of the U.S.* (D. Mass 2005) 396 F.Supp.2d 45, 48 ["the information contained in the 'subject' would reveal the contents of the communication"]; Orin S. Kerr, *A User's Guide to the Stored Communications Act*, (2004) 72 Geo. Wash. L. Rev. 1228 ["the subject line generally carries a substantive message"].

In contrast, "records" consist of raw data that is merely ancillary to the communication.[25] Examples include the "to/from" names and addresses, dates, and times pertaining to an email message, the phone numbers that were transmitted to telephone switching equipment, the addresses of websites that were visited on a certain computer, and the internet or IP address assigned to a particular computer.[26] While it is true that such raw data might permit officers to draw some conclusions as to a person's interests or other private matters, it will ordinarily be deemed a "record"—not a "communication." As the Ninth Circuit explained in *U.S.* v. *Forrester*:

> When the government obtains the to/from addresses of a person's e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed. At best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses and IP addresses—but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed. Like IP addresses, certain phone numbers may strongly indicate the underlying contents of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms. Further, when an individual dials a prerecorded information or subject-specific line, such as sports scores, lottery results or phone sex lines, the phone number may even show that the caller had access to specific content information. Nonetheless, the [Supreme Court has drawn] a clear line between unprotected addressing information and protected content information . . .[27]

It should be noted, however, that while the locations of websites a person visited are considered records, it is possible, that Uniform Resource Locators (URLs) will be deemed content because they indicate "the location of specific documents on the Web" that a person has viewed and, thus, constitute the type of "personal information" that may be entitled to greater protection.[28]

How to Obtain Communications

Now we get to the heart of the matter: How can officers obtain copies of email, voicemail, and text messages from providers? As we will discuss, there are five ways, but only one of them—a search warrant—has much practical importance in California.

SEARCH WARRANTS: In most cases, officers should seek a search warrant if they have probable cause to believe that certain email, voicemail, or text messages constitute evidence of a crime. There are four reasons for this:

(1) REQUIRED FOR NEW MESSAGES: The SCA requires a warrant if, as is usually the case, officers want to search for messages that have been in storage for 180 days or less.[29]

(2) AUTHORIZED BY CALIFORNIA LAW: The California Penal Code expressly authorizes the issuance of search warrants for this purpose.[30]

(3) PROVIDER MAY REQUIRE IT: Although the SCA permits the release of communications by means of a subpoena or a D-Order (discussed below), some providers insist upon search warrants so as to eliminate any possibility of liability resulting from disclosure.

(4) THE JUDGE MAY REQUIRE IT: Because the law in this area is somewhat inarticulate (especially the sufficiently of D-Orders), some judges have refused to authorize the release of electronic communications by any means other than a search warrant.

---

[25] See *Smith* v. *Maryland* (1979) 442 U.S. 735. 741 ["Yet a pen register differs significantly from [a listening device] for pen registers do not acquire the *contents* of communications."].

[26] See *In re § 2703(d) Order* (E.D. Va. 2011) 787 F.Supp.2d 430, 436 ["The Twitter Order does not demand the contents of any communication, and thus constitutes only a request for records"].

[27] (9th Cir. 2008) 512 F.3d 500, 510.

[28] See *In re Pharmatrak Privacy Litigation* (1st Cir. 2003) 329 F.3d 9, 13, 16.

[29] See 18 U.S.C. § 2703(a); *U.S.* v. *Warshak* (6th Cir. 2011) 631 F.3d 266, 283 ["The government may obtain the contents of e-mails that are in electronic storage with an electronic communications service for 180 days or less only pursuant to a warrant."].

[30] Pen. Code § 1524.2.

Furthermore, in a decision that has drawn a lot of discussion, the Sixth Circuit ruled in *United States.* v. *Warshak*[31] that, while the Stored Communications Act permits the acquisition of email by means of a D-Order, the Fourth Amendment does not. The court reasoned that people who communicate via email can and do reasonably expect that their communications will remain private. And this means that the release of these communications to law enforcement is governed by the Fourth Amendment (in addition to the SCA). Consequently, as in most intrusions that are deemed "searches," a warrant will be required unless there is an exception to the warrant requirement, such as emergency or consent. Said the court:

> It only stands to reason that, if government agents compel an [internet service provider] to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception.[32]

Commenting on this ruling, CNET.com said, "The decision, assuming it survives a potential appeal to the U.S. Supreme Court, marks a major turning point in the evolution of Fourth Amendment law in the Digital Age."[33]

Two other things should be noted about *Warshak*. First, the Ninth Circuit has indicated it agrees with the court's analysis.[34] Second, while decisions of the federal circuits courts are not binding on California courts, a well-reasoned case such as *Warshak* may have substantial persuasive value.[35]

There are some other things about search warrants that should be noted:

NO NOTICE TO SUBSCRIBER: Officers are not required to notify the subscriber that a warrant for his communications or records was executed.[36]

NOTICE TO PRESERVE: Because providers routinely delete email and other stored electronic communications, and also because subscribers may be able to delete their own messages, the SCA provides that ISPs must preserve these messages for 90 days if officers request them to do so.[37] Accordingly, when officers determine that voicemail, email, or text messages may be relevant to an investigation, they should immediately contact the provider, give notice that a warrant will be sought, and request that they save any stored messages.

PRESERVATION REQUIRED: A provider who receives a preservation request must "take all necessary steps to preserve records and other evidence in its possession," and must retain it for 90 days.[38] A 90-day extension must be granted if officers request it.

NONDISCLOSURE ORDERS: If an investigation would be jeopardized if the suspect knew that officers had obtained copies of his email, voicemail, or text messages, officers may seek a nondisclosure order prohibiting the service provider from releasing this information to the customer for 90 days.[39] Grounds for a such an order will exist if officers reasonably believed that disclosure would (1) endanger the life or safety of a person, (2) result in flight from prosecution, (3) result in destruction of or tampering with evidence, (4) result in the intimidation of a potential witness, or (5) would otherwise seriously jeopardize the investigation or unduly delay a trial.[40] A court may order 90-day extensions of a nondisclosure order.[41]

---

[31] (6th Cir. 2010) 631 F.3d 266, 286.
[32] But also see *Rehberg* v. *Paulk* (11th Cir. 2010) 611 F.3d 828, 847 ["No Supreme Court decision and no precedential decision of this Circuit defines privacy rights in email content voluntarily transmitted over the global Internet and stores at a third-party ISP."].
[33] Larry Downes, "Search warrants and online data: Getting real," CNET News (December 15, 2010).
[34] See *U.S.* v. *Forrester* (9th Cir. 2008) 512 F.3d 500, 511 ["The privacy interests in these two forms of communication [i.e., email and physical mail] are identical."].
[35] See *People* v. *Bradford* (1997) 15 Cal.4th 1229, 1305 ["Such decisions, as we often have observed, provide persuasive rather than binding authority."].
[36] See Pen. Code § 1524.3(b) ["A governmental entity receiving subscriber records or information [by means of a search warrant] is not required to provide notice to a subscriber or customer."].
[37] See 18 U.S.C. § 2703(f).
[38] See Pen. Code § 1524.3(d); 18 USC § 2703(f).
[39] See 18 U.S.C. §2705(a)(1).
[40] See 18 USC § 2705(a)(2).
[41] See 18 U.S.C. 2705(a)(4)

WARRANTS ON OUT-OF-STATE ISPS: A judge in California may issue a search warrant for records stored in another state if the provider is doing business here.[42]

SERVING CORPORATIONS: A warrant for stored communications in the possession of a California corporation and most out-of-state corporations may be served by means of U.S. mail, overnight delivery service, fax, or hand delivery to (1) any officer or general manager located in California, or (2) its agent for service of process.[43] It is also a good idea to send a copy of the warrant to the provider's law enforcement liaison, if any. Note that the Penal Code requires that foreign corporations produce the requested communications within five business days of receipt, although the judge may require the production of such communications in less than five days if investigators establish good cause, such as a danger to life or flight from prosecution.[44]

REIMBURSEMENT: A law enforcement agency that obtains email, voicemail, or text messages from a service provider by means of a search warrant or otherwise must reimburse the company "for such costs as are reasonably necessary, and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information."[45]

D-ORDERS: The SCA states that officers may, under certain circumstances, obtain copies of email, voicemail, and text messages by means of a court order, commonly known as a "2703(d) Order" or simply a "D-Order." The advantage of a D-Order is that it does not require probable cause. Instead, a court may issue such an order if the accompanying application contains "specific and articulable facts" that establish "reasonable grounds" to believe that the contents of the communication "are relevant and material to an ongoing criminal investigation."[46] One disadvantage of D-Orders is that officers must ordinarily give the subscriber notice that they will be seeking one so that he may obtain judicial review.[47]

D-Orders are, however, controversial because they permit the release of private communications on less than probable cause. Thus, judges may not issue them. Furthermore, when we went to press the U.S. Senate was considering a bill that would generally prohibit the release of such communications except by means of a search warrant.

SUBPOENA: Although the SCA also permits the release of electronic communications by means of subpoena, the subpoena procedure in California is so restrictive that, as a practical matter, subpoenas are seldom useful.[48]

CONSENT: An ISP may release copies of an email, voicemail, or text message to officers if the sender or recipient consented to the release in writing.[49]

EMERGENCIES: The SCA permits providers to voluntarily disclose stored communications to law enforcement officers if (1) the provider "in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay," (2) the disclosure is made "to the National Center for Missing and Exploited Children, in connection with a report submitted thereto" under 42 U.S.C. §13032, or (3) the provider learned of the communication "inadvertently" and determined that it pertained "to the commission of a crime."[50] POV

---

[42] See Pen. Code § 1524.2; Code Civ. Proc. § 410.10; Corp. Code § 2105(a)(5); *People* v. *Stipo* (2011) 195 Cal.App.4th 664, 671.
[43] See Pen. Code § 1524.2(a)(6); Corporations Code § 2110; 18 USC § 2703(g).
[44] See Pen. Code § 1524.2.
[45] See 18 U.S.C. § 2706.
[46] 18 U.S.C. § 2703(d).
[47] See 18 USC § 2703(b)(1)(B)(ii).
[48] See Pen. Code §§ 1326, 1327; Evid. Code § 1560; *People* v. *Superior Court (Barrett)* (2000) 80 Cal.App.4th 1305, 1315 [a subpoena duces tecum requires the person served "to produce information in court"]; *Carlson* v. *Superior Court* (1976) 58 Cal.App.3d 13, 22 ["[L]aw enforcement officials may not gain access to an accused's private papers by subpoena until there has been a judicial determination there is probable cause to believe he has committed a criminal offense and that the papers [are evidence]."].
[49] See 18 U.S.C. § 2702(b)(3); *S.E.C.* v. *Jerry T. O'Brien, Inc.* (1984) 467 U.S. 735, 743 [an ISP may divulge the contents of an email "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service"].
[50] See 18 U.S.C. § 2702(c).

Electronic Communication Records
Telephone, Email, and Internet

In Scott Peterson's murder trial, Peterson's cell phone records were introduced to establish his whereabouts on the morning of his wife's murder, belying his version of the events of that morning.[1]

Every day, virtually every criminal in the U.S. (at least those who aren't incarcerated) will use a phone, send or receive email, surf the internet, or all four. So it is not surprising that many of the records pertaining to these communications can help investigators solve crimes and assist prosecutors in obtaining convictions. Among other things, they may reveal the identities of the suspect's accomplices, establish the dates and times of their contacts, and prove the suspect's whereabouts when a crime occurred. As the California Supreme Court observed, "[A] record of telephone calls provides a virtual current biography."[2] In fact, electronic communication records now permit officers to follow a suspect by obtaining realtime reports of the locations of the cell phone towers that are receiving signals from his phone.

The question, then, is what are the legal requirements for obtaining these records? Unfortunately, the answer is not crystal clear. And the reason is the same as the reason that officers are having trouble figuring out the rules for obtaining copies of the communications themselves (which was the subject of the previous article). Simply put, both subjects are regulated by a federal law that was badly written and poorly organized, and which has not kept pace with changes in technology.

Another consequence of this uncertainty is that overcautious service providers sometimes demand legal process beyond that required by the law. As a result, officers who have complied with all the legal requirements will sometimes be told by the provider that it's not enough. And this can result in delays that seriously impair investigations.

For example, homicide investigators in Hayward obtained a search warrant for a murder victim's AT&T records and voicemail. They needed this information because they had virtually no leads in the case and they thought it would help if they knew the identities of the people who recently spoke with the victim. But AT&T refused to turn over the records or tapes unless the officers obtained a *wiretap* order. We challenged this in court, and won. But the incident cost time and money, and it needlessly delayed the investigation.

Nevertheless, it is possible to make sense of this area of the law, and that is the purpose of this article. But before we begin, there are four things that should be noted. First, there is a significant difference between communications (or "content") and records, although a summary will suffice here because we discussed this issue at length in the accompanying article. A communication is the message that was sent or received, while a record consists of information that is ancillary or incidental to its transmission, such as information about the subscriber, the phone numbers and email addresses of the senders and recipients of messages, and exactly when those messages were made or received.[3]

Second, the rules for obtaining copies of electronic communication records are set forth in the federal Electronic Communications Privacy Act (ECPA). In particular, the section known as the Stored Communications Act (SCA) covers the acquisition of subscriber and transaction records,[4] while data pertaining to pen registers and connection traps are covered in a separate chapter which also (arguably) covers the means by which officers can obtain cell tower location records.[5]

Third, although the ECPA covers both the disclosure of content and records, the requirements for obtaining records are not as strict as those pertain-

[1] Samuel, Ian J., Warrantless Location Tracking. New York Univ. Law Rev., Vol. 83, No. 4, October 2008 at p. 1324.
[2] *People* v. *Blair* (1979) 25 Cal.3d 640, 653.
[3] See *Smith* v. *Maryland* (1979) 442 U.S. 735, 741; *In re application for digital analyzer* (C.D. Cal. 1995) 885 F.Supp. 197, 199.
[4] 18 U.S.C. § 2701-2712.
[5] 18 U.S.C. § 3121-3127.

ing to content. This is because people know that the records of their communications are routinely read by employees of the provider, or are at least readily accessible to them when, for example, the subscriber calls the provider with questions about his account.[6] As we will discuss later, however, this area of the law may be changing as to records that reveal information that is deemed too private to be subject to the less restrictive rules.

Fourth, we will email the following forms to officers and prosecutors (in Microsoft Word format which can be edited) if they send a request from a departmental email address to POV@acgov.org:

- Search warrant for communication records*
- Court order for communication records*
- Court order for telephone transaction records
- Emergency declaration

Subscriber Records

Of all the communication records that investigators may need, the least private are subscriber records which consist essentially of data pertaining to the subscriber's identity, his address, the equipment and services he utilizes, and his payment records.[7] Thus, the SCA defines "records" as including the subscriber's name, address, "length of service (including start date) and types of service utilized," "telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address," and the "means and source of payment for such service (including any credit card or bank account number)."[8]

Although worded differently, the Penal Code's definition of electronic communication records is essentially the same, as it consists of "the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to or customer of that service, and the types of services the subscriber or customer utilized."[9]

Because this information is not considered highly private (even as to unlisted phone numbers[10]), officers can obtain it in several ways, as follows:

SEARCH WARRANT: If investigators have probable cause, they will usually seek subscriber records by means of a search warrant. This is mainly because both federal and California law expressly authorize it.[11] For information on how to obtain and execute these warrants, see the discussion on pages 5-8.

D-ORDER: Federal law also permits California judges to authorize the release of certain communication records by means of a court order, commonly known as a "D-Order." Although probable cause is not required, the applicant must submit a declaration containing "specific and articulable facts" demonstrating reasonable grounds to believe that the records are "relevant and material to an ongoing criminal investigation."[12] There are, however, three reasons that investigators should consider seeking a search warrant instead of a D-Order. First, as a practical matter, there is not much difference between the two standards of proof. Second, California law does not expressly authorize state judges to issue D-Orders.[13] Third, because officers and judges are more familiar with the search warrant procedure, a warrant may be less time-consuming.

---

* Copies of these forms are on pages 15 and 16.

[6] See *Smith* v. *Maryland* (1979) 442 U.S. 735, 743 ["it is too much to believe that telephone subscribers harbor any general expectation that the numbers they dial will remain secret"]; *People* v. *Stipo* (2011) 195 Cal.App.4th 664, 669 ["Analogously, e-mail and Internet users have no expectation of privacy in the . . . IP addresses of the websites they visit"]; *In re § 2703(d) Order* (E.D. Va. 2011) 787 F.Supp.2d 430, 440 ["[P]etitioners in this case voluntarily conveyed their IP addresses to the Twitter website . . . thereby relinquishing any reasonable expectation of privacy."].

[7] See *People* v. *Lissauer* (1985) 169 Cal.App.3d 413, 419 ["the police did not require a warrant to obtain appellant's name and address from the telephone company"]; *U.S.* v. *Perrine* (10th Cir. 2008) 518 F.3d 1196, 1204 ["Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation."].

[8] 18 U.S.C. 2703(c)(2).

[9] Pen. Code § 1524.3(a); 18 U.S.C. 2703(c)(1)(A).

[10] See *People* v. *Lissauer* (1985) 169 Cal.App.3d 413, 419.

[11] Pen. Code § 1524.3(a).

[12] See 18 U.S.C. § 2703(d).

[13] **NOTE**: Technically, it is immaterial that California law does not expressly authorize the issuance of D-Orders because, per 18 U.S.C. § 2703(d), state judges may issue D-Orders unless *prohibited* by state law. And there is no law in California that prohibits the issuance of D-Orders.

CONSENT: Officers can obtain a subscriber's records if the subscriber gives written consent.[14]
EMERGENCY NOTIFICATION: Providers are required to disclose communication records if officers notify them that such disclosure was reasonably necessary to forestall "an emergency involving danger of death or serious physical injury."[15] As noted earlier, officers can obtain an emergency notification form by sending a request from a departmental email address to POV@acgov.org.
COURT ORDER: MONEY LAUNDERING OR FRAUD: The Penal Code authorizes judges to issue court orders for certain records if the crime under investigation was money laundering or if it consisted of multiple counts of particular types of fraud or embezzlement.[16]

Transaction Records

In contrast to subscriber records, transaction records consist of data pertaining to the subscriber's *use* of electronic communications services.[17] For example, telephone records would include local and long distance connection data, records of session times, and the duration of calls. Similarly, email transaction records would include "to/from" names and addresses, and the dates and times that messages were sent or received. As for internet records, they consist of the internet protocol (IP) addresses of a person's computer[18] and the websites that were visited by that computer, including the date and time of the visits.[19] Transaction records can be obtained by the same procedures that are used to obtain subscriber records.[20]

Note that some information in a transaction record may be deemed "content," such as the "subject" line in an email, and the specific pages on a website that were accessed by a certain computer; i.e., URLs.[21] But this will not ordinarily present a problem because most of the procedures by which investigators can obtain subscriber and transaction records may also authorize the release of content.[22]

Pen Registers and Connection Traps

"Pen registers" and "connection traps" are devices or software applications that record the phone numbers, email addresses, and web sites to which a target phone, computer, or other device has established a connection. Specifically, pen registers record data pertaining to outgoing calls and messages (e.g., phone numbers dialed, email addressees), while connection traps (also known as "trap and trace" devices) record incoming data.[23] (The terms pen register and connection trap are holdovers from the days when they were instruments that phone companies would attach to their switching equipment. Now the job is ordinarily done by computers.)

---

[14] See 18 U.S.C. §§ 2702(c)(2), 2703(c)(1)(c).
[15] 18 U.S.C. § 2702(c)(4).
[16] See Pen. Code § 1326.1.
[17] See 18 U.S.C. § 2703(c)(2); Pen. Code § 1524.3(a) ["toll billing records"].
[18] See *People* v. *Stipo* (2011) 195 Cal.App.4th 664, 669; *U.S.* v. *Forrester* (9th Cir. 2008) 512 F.3d 500, 510 ["Internet users have no expectation of privacy in the . . . IP addresses of the websites they visited because they should know that this information is provided to and used by Internet service providers for the specific purpose directing the routing of information."]. Also see *In re Pharmatrak* (1st Cir. 2003) 329 F.3d 9, 13, fn.1 ["An IP address is the unique address assigned to every machine on the internet. An IP address consists of four numbers separated by dots, e.g., 166.132.78.215."]; *U.S.* v. *Forrester* (9th Cir. 2008) 512 F.3d 500, 510, fn.5 ["Every computer or server connected to the Internet has a unique IP address."].
[19] See *U.S.* v. *Allen* (C.A.A.F. 2000) 53 M.J. 402, 409 [the information obtained from defendant's ISP was merely a "record" because it was limited to "a log identifying the date, time, user, and detailed internet address of sites accessed"].
[20] See 18 U.S.C. §§ 2702(c), 2703(c)(2)(C).
[21] See *In re Pharmatrak Privacy Litigation* (1st Cir. 2003) 329 F.3d 9, 13, fn.2 ["URLs (Uniform Resource Locators) are unique addresses indicating the location of specific documents on the Web. The webpage a user viewed immediately prior to visiting a particular website is known as the referrer URL. Search engines such as Yahoo! are common referrer URLs."].
[22] See 18 U.S. C. §§ 2702-2703.
[23] See 18 U.S.C. § 3127(3) ["the term 'pen register' means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted"]; 18 U.S.C. § 3127 (4) ["the term 'trap and trace device' means "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication"].

How to obtain authorization

There are three ways in which officers and prosecutors can obtain data by means of a pen register or connection trap.

SEARCH WARRANT: A judge may authorize the use of a pen register or connection trap by means of a search warrant if the supporting affidavit establishes probable cause to believe the data "tends to show a felony has been committed, or tends to show that a particular person has committed a felony,"[24] or if it "tends to show that sexual exploitation of a child" had occurred.[25]

Although it may be somewhat easier to obtain pen register and connection trap data by means of a Pen-Trap Order (discussed next), there are two reasons that investigators might seek a warrant. First, a warrant can also authorize the phone company or ISP to provide the names and addresses of the people who sent or received the phone calls or emails; and in most cases this information is essential. Second, there is an opinion by the California Attorney General which asserts that California judges do not have the authority to issue Pen-Trap Orders.[26] As we explained in the Spring 2004 edition of *Point of View*, there is reason to believe that this opinion is mistaken. Still, it has added to the uncertainty that surrounds this subject and, as a result, judges may insist on search warrants.

PEN-TRAP ORDER: A Pen-Trap Order is the least demanding type of court order in this field because officers need only submit an application containing the following: (1) the name of the applicant and his law enforcement agency, and (2) a declaration under penalty of perjury that the information that is likely to be obtained by means of a pen register or connection trap "is relevant to an ongoing criminal investigation."[27] Thus, unlike a search warrant, officers need not explain *why* the information is needed. As the court pointed out in *In re Application of the United States*:

> The court is not asked to "approve" the application for a pen register in the sense that the court would vouch initially for the propriety of the use of a wiretap. Congress asks the court only to confirm that the approved safety measures are observed—that is, primarily, that the responsible persons are identified and accountable if any malfeasance or misprision comes to light.[28]

In determining whether to seek a Pen-Trap Order or a search warrant, officers and prosecutors should keep the following in mind:

(1) PROBABLE CAUSE IS NOT REQUIRED. As noted, a Pen-Trap Order merely requires a declaration that the records would be relevant to an ongoing investigation (which would include misdemeanors). In contrast, a search warrant requires that officers set forth facts establishing probable cause to believe that the information is evidence of a felony.

(2) LONGER MONITORING: A judge who issues a Pen-Trap Order may authorize monitoring for up to 60 days (and extensions of up to 60 days[29]), while a search warrant is void after ten days.[30]

(3) SIMPLE PROCEDURE: Federal law has established a quick and easy procedure for obtaining Pen-Trap Orders.[31] For example, they are automatically sealed and they include a nondisclosure order prohibiting the provider from informing the subscriber that the order was received.[32] Also, officers can obtain an extension by simply submitting another application; i.e., they need not explain why an extension was necessary, or explain what information had been obtained to date.[33]

---

[24] See Pen. Code § 1524(a)(4).
[25] See Pen. Code § 1524(a)(5).
[26] 86 Ops. Cal. Atty. Gen. 198.
[27] 18 U.S.C. § 3123(a)(2). ALSO SEE *U.S.* v. *Fregoso* (8th Cir. 1995) 60 F.3d 1314, 1320.
[28] (M.D. Fla. 1994) 846 F.Supp. 1555, 1561.
[29] See 18 U.S.C. § 3123(c)(1)(2); *People* v. *Larkin* (1987) 194 Cal.App.3d 650, 656-57.
[30] See Pen. Code § 1534(a).
[31] See *In re application of the U.S.* (M.D. Fla. 1994) 846 F.Supp. 1555, 1559 ["The procedure for obtaining authorization for a pen register is summary in nature and the requisite disclosure is perfunctory."].
[32] See 18 U.S.C. § 3123(d).
[33] See *In re application of the U.S.* (M.D. Fla. 1994) 846 F.Supp, 1555, 1560.

EMERGENCY DECLARATION: A provider will immediately install a pen register or connection trap and start furnishing officers with the data upon receipt of a declaration that such data is needed as a result of any of the following: (1) an immediate danger of death or serious bodily injury to any person, (2) conspiratorial activities characteristic of organized crime, (3) an immediate threat to a national security interest, or (4) an ongoing attack (punishable as a felony) on a protected computer (as defined in 18 U.S.C. § 1030).[34]

Cell Phone Location Records

Cell phone location records provide investigators with the location of cell phone transmission towers that (1) received automatic location-monitoring "pings" from a certain phone,[35] or (2) transmitted communication signals to or from the phone. These records also typically include the date, time, and duration of the transmission. Such information can be important because it constitutes circumstantial evidence that a suspect, victim, or other person was at or near a certain location at a particular time.[36]

There are two types of cell phone location records: "historical" and "prospective." Historical records are those pertaining to transmissions received in the past. For example, in order to determine the whereabouts of Scott Peterson on the day his wife disappeared, investigators in Modesto obtained historical cell site data for that day. In contrast, if investigators wanted to follow a suspect by monitoring his cell phone transmissions, they would seek prospective data; e.g., realtime reports that are sent to them directly.

Developments in the law

The acquisition of cell site location records is one of the hottest topics in the law today. This is because such data can provide officers with substantially more information than just the general location of a certain phone. In fact, depending on the technology in use by the subscriber and provider, officers may be able to determine its exact location and generate a detailed map of the subscriber's travels. This can be accomplished by means of triangulation if the signal was received by multiple towers,[37] or by GPS technology if the suspect was using a phone that had been upgraded to "Enhanced 911" standards.[38]

Also under discussion is the extent to which a person's privacy may be invaded if officers use these records to track him for a substantial amount of time—say, weeks or months. This issue is now before the Supreme Court which may rule shortly.[39]

Not surprisingly, these developments have sparked a lot of controversy and have become highly newsworthy. As the D.C. Circuit observed:

---

[34] See *United States* v. *New York Telephone Co.* (1977) 434 U.S. 159, 168-70; 18 U.S.C. § 3125(a). Also see Pub. Util. Code § 2891(d)(5) [incoming and outgoing phone numbers may be given to a law enforcement agency responding to a 911 telephone call or any other call communicating an imminent threat to life or property]. **NOTE**: Federal law requires that the person who declares the emergency must be specifically authorized to do so by the California Attorney General, certain California Department of Justice administrators, or the principal prosecuting attorney of a county or city. 18 U.S.C. 3125(a).

[35] See *In re Application of U.S.* (S.D.N.Y. 2006) 460 F.Supp.2d 448, 450 ["Whenever a cellular telephone is in the 'on' condition, regardless of whether it is making or receiving a voice or data call, it periodically transmits a unique identification number to register its presence and location in the network. That signal, as well as calls made from the cellular phone, are received by every antenna tower within range of the phone."].

[36] See, for example, *People* v. *Martin* (2002) 98 Cal.App.4th 408, 412 [cell tower contacts were used to establish the defendant's location when the victim was murdered].

[37] See *In re Application of the United States* (S.D.N.Y. 2006) 460 F.Supp.2d 448, 452 ["Where the government obtains information from multiple towers simultaneously, it often can triangulate the caller's precise location and movements by comparing the strength, angle, and timing of the cell phone's signal measured from each of the sites."]; *In re Application of the United States* (3d Cir. 2010) 620 F.3d 304, 308 [data included "which of the tower's 'faces' carried a given call at its beginning and end"].

[38] See *In re Application of the United States* (3d Cir. 2010) 620 F.3d 304, 311 [the Government notes that "much more precise location information is available when global positioning system ('GPS') technology is installed in a cell phone"]. **NOTE**: Phase II of the FCC's wireless 911 rules "require wireless service providers to provide more precise location information to PSAPs; specifically, the latitude and longitude of the caller. This information must be accurate to within 50 to 300 meters depending upon the type of location technology used." Federal Communications Commission, "Wireless 911 Services," www.fcc.gov/guides/wireless-911-services. Accessed September 2011.

[39] See *United States* v. *Jones* (2011) 131 S.Ct. 3064.

> The use of and justification for cell phone tracking is a topic of considerable public interest: it has received widespread media attention and has been a focus of inquiry in several congressional hearings considering, among other things, whether [federal law] should be revised either to limit or to facilitate the practice.[40]

More recently, *The Wall Street Journal* published a front-page story about the FBI's "Stingray" cellphone surveillance project under the headline: "'Stingray' Phone Tracker Fuels Constitutional Clash."

In addition to privacy concerns, this subject is generating considerable interest because there are no federal rules that expressly govern the release of cell phone location data to law enforcement. As one circuit court put it, "[W]e are stymied by the failure of Congress to make its intention clear."[41] One consequence of this failure is that federal prosecutors have had to justify the warrantless acquisition of cell tower data by resorting to inferences from language in the statutes that regulate pen registers and connection traps.

Meanwhile, legal scholars, privacy advocates, and law enforcement officials are engaged in a debate as to whether Congress should address the matter and, if so, what standards it should adopt. Thus, a writer for the New York University Law Review observed that "[t]he question is not *whether* the government can obtain cell site information, but rather what *standard* it must meet before a court will authorize such disclosure."[42] More to the point, the question is whether officers must have probable cause or whether some lesser standard of proof would be adequate.

This is an especially significant issue for federal investigators and prosecutors because, if probable cause is not required, they can readily utilize the federal administrative subpoena procedure which requires mere relevance. But for state and local investigators and their agencies, this issue may not be as important because they will seldom expend the resources necessary to embark on a cell site surveillance project unless they have a minimum of probable cause, in which case they can readily obtain a search warrant.

In any event, the following requirements are now under consideration:

(1) **SEARCH WARRANT**: It is apparent that, whatever standards are eventually adopted, officers will be able to obtain cell phone location data by means of a search warrant based on a showing of probable cause. In fact, when we went to press the U.S. Senate was considering a bill that would require a search warrant to conduct realtime cell phone tracking.

(2) **D-ORDER BASED ON PROBABLE CAUSE**: Some federal magistrates have advocated a rule that would permit the release of cell site location data by means of a D-Order (discussed on pages 7 and 9), except that this particular D-Order would require probable cause.[43] But because such a hybrid court order would be virtually indistinguishable from a search warrant, and also for the reasons discussed on page 14, this option would not be of much use to state and local investigators.

(3) **D-ORDER BASED ON RELEVANCE + SPECIFIC FACTS**: Opponents of a probable-cause requirement have suggested that cell tower data should be obtainable by means of a hybrid D-Order that would be issued if the applicant set forth specific facts demonstrating that the data would be relevant to an ongoing criminal investigation. This standard of proof might be considered a workable compromise.

(4) **D-ORDER BASED ON RELEVANCE**: The lowest standard of proof for obtaining this data is a court order that, like a Pen-Trap Order, would require only a declaration that the information would be relevant to an ongoing criminal investigation. This is probably a nonstarter.

It is possible (maybe even likely) that the required level of proof—whether it is probable cause or something less—will vary depending on the following circumstances:

---

[40] *ACLU* v. *U.S. Department of Justice* (D.C. Cir. 2011) 635 F.3d 1, 12-13.
[41] *In re Application of the United States* (3d Cir. 2010) 620 F.3d 304, 319.
[42] Samuel, Ian J., Warrantless Location Tracking. New York Univ. Law Rev., Vol. 83, No. 4, October 2008 at p. 1333.
[43] See *In re Application of the United States* (3d Cir. 2010) 620 F.3d 304, 310, fn.6.

- **GENERAL OR SPECIFIC LOCATION?** Whether the data was obtained by means of single-tower contacts, or whether it revealed the suspect's exact whereabouts or route by means of triangulation or GPS.
- **HISTORICAL OR PROSPECTIVE?** Whether officers were seeking historical or prospective data.
- **DURATION**: The duration of the surveillance. (This will be especially important if officers are seeking prospective data.)

Consequently, it has been argued that officers should be able to obtain historical data based on something less than probable cause, while a search warrant or D-Order based on probable cause would be required to obtain prospective (i.e., realtime) data. In fact, there is one case involving historical data in which the court ruled that a D-Order would suffice, and that a court may issue a D-Order if officers set forth facts that establish that the information would be relevant to an ongoing criminal investigation.[44] The court's reasoning was sound: it pointed out that the Supreme Court has ruled that people who walk or drive in public places cannot ordinarily expect that their movements will not be observed by others.[45] And, so long as cell phone data does nothing more than provide officers with this information, probable cause should not be required.

As for prospective data, the U.S. Department of Justice has argued that it should be obtainable by means a D-Order based on "reasonable grounds" to believe that the data is "relevant and material to an ongoing criminal investigation."[46]

Unfortunately, California courts have not yet had to address these issues, and the few federal district courts that have are split on the question.[47] As one commentator observed, "[T]here is a live statutory disagreement amongst judges regarding an enormously important tool used in police investigations, a disagreement whose contours cannot even be fully mapped by a close study of the published opinions."[48]

We may, however, get a better read on this issue when the United States Supreme Court decides the case of *United States* v. *Jones* early this year.[49] In *Jones*, the Court is expected to rule on whether officers need a search warrant to use a tracking device to follow a vehicle on public streets for an extended period of time. This might affect cell site location disclosure because it is arguable that prospective cell site location records function as "tracking devices" which would require a search warrant under federal law.

How to obtain cell site data

Until the issue is settled, state and local investigators and prosecutors should probably seek a search warrant to obtain cell site location data, especially if they are seeking prospective data. Although it is possible that a D-Order based on mere relevance will suffice, the savings in time and effort will almost always be outweighed by other considerations, such as uncertainty as to whether a judge will sign the order, the delay that frequently results when a judge must research an unsettled area of law, and the possibility of a reversal on appeal. Furthermore, the standard of proof for a D-Order is almost indistinguishable from that of a search warrant, as officers would still be required to explain why the records they are seeking would be relevant to their investigation.

It should also be noted that, by obtaining a search warrant instead of a subpoena or D-Order, officers who are receiving realtime location records can continue their surveillance if the suspect enters his home or other place in which he has a reasonable expectation of privacy. POV

---

[44] *In re Application of the United States* (3d Cir. 2010) 620 F.3d 304, 308. Also see *In re Application of the United States* (S.D.N.Y. 2006) 460 F.Supp.2d 448, 460-61.

[45] Citing *United States* v. *Knotts* (1983) 460 U.S. 276; *United States* v. *Karo* (1984) 468 U.S. 705.

[46] See Computer Crime and Intellectual Property Section [of DOJ], "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" (Chapter 4 Electronic Surveillance in Communication Networks), www.cybercrime, gov/ssmanual/03ssma.html, accessed September 2011.

[47] See, for example, *In re Application of the U.S.* (3d Cir. 2010) 620 F.3d 304, 310, fn.6 ["Some of those cases hold that the government cannot obtain prospective, i.e., realtime [data] through the 'hybrid' theory" but others hold they may. Citations omitted.].

[48] Samuel, Ian J., Warrantless Location Tracking. New York Univ. Law Rev., Vol. 83, No. 4, October 2008 at p. 1329.

[49] (2011) 131 S.Ct. 3064.

SUPERIOR COURT OF CALIFORNIA
County of _____

SEARCH WARRANT
Electronic Communication Records
18 U.S.C. §2703(c)(1)(A), Penal Code § 1524.3(a)

The Great Seal

THE PEOPLE OF THE STATE OF CALIFORNIA
to any peace officer in _____ County: Warrant No. _____

An affidavit, sworn to and subscribed before me on this date, has established probable cause for this search warrant which you are ordered to execute as follows:

PLACE TO BE SEARCHED: [Insert name and address of provider], hereinafter "Provider."
Subscriber: [Insert available information; e.g. name, address, phone number, e-mail address, Internet Protocol (IP) address]
Type of service provided: ☐ Telephone ☐ Email ☐ Internet

RECORDS TO BE SEIZED

Specific records

☐ Subscriber's name and address
☐ Telephone number, email address, IP address
☐ Means and source of payment, including credit card and bank account numbers
☐ Types of services utilized
☐ Length of service, including start date

Connection records

Telephone

☐ Local and long distance connection records from _____to _____
☐ Last outgoing phone number ☐ Last incoming phone number

Email and Internet

☐ Email or IP address of the person or computer contacted, session times, and duration of sessions from _____to _____

Other records: [Specify]

COMPLIANCE DATE: Provider shall furnish the listed records to the affiant on or before _____.

FINDINGS

(1) Provider is a California corporation or a foreign corporation doing business in California, and is a provider of electronic communication service as defined in 18 USC § 2510(15) and Penal Code § 1524.2(a)(1).

(2) Pursuant to 18 USC §§ 2703(c)(1)(A) and Penal Code § 1524.2(b), 1524.3, upon a showing of probable cause this court is authorized to issue this search warrant for the records listed above.

(3) The affidavit filed herewith, which was sworn to and subscribed before me on this date, has established probable cause to believe the records listed above are in the possession of Provider and that they [check applicable]
☐ Tend to show a felony has been committed or tend to show that a particular person has committed a felony.
☐ Tend to show that sexual exploitation of a child (Penal Code § 311.3), or possession of matter depicting sexual conduct of a person under the age of 18 years (Penal Code § 311.11) has occurred or is occurring.

SEALING ORDER: Pending further order of this court, this search warrant and all accompanying documents shall not become a public record and shall be sealed and delivered into the custody of the Clerk of the Superior Court.
Grounds for sealing: ☐ Informant protection (Evid. Code § 1041) ☐ Official information (Evid. Code § 1040)

NON-DISCLOSURE ORDER: Provider shall not notify Subscriber or any other person of the existence or content of this search warrant pending further order of this court.

_____ _____
Date Judge of the Superior Court

SUPERIOR COURT OF CALIFORNIA

County of _____

COURT ORDER

Electronic Communication Records

18 U.S.C. § 2703(d)

The Great Seal

To: [Insert name of provider], hereinafter "Provider"

Type of Service Provided: ☐ Telephone ☐ Email ☐ Internet

Applicant: [Insert name of applicant and agency], hereinafter "Applicant."

Subscriber: [Insert available information; e.g., name, address, phone number, email address, IP address]

Order: Based on the findings below, Provider is ordered to furnish Applicant with the following records if they are in Provider's possession or Provider can obtain them with reasonable effort:

Subscriber Records

☐ Subscriber's name and address ☐ Types of services utilized

☐ Telephone number, email address, IP address ☐ Length of service, including start date

☐ Means and source of payment, including credit card and bank account numbers

Connection Records

Telephone

☐ Local and long distance connection records from _____ to _____

☐ Last number dialed ☐ Phone number of last incoming call

Email and Internet

☐ Email or IP address of person or computer contacted, session times, duration of sessions from: [insert dates].

Other Records: [Specify]

Compliance Date: Provider shall furnish the listed records to Applicant on or before [insert date].

Compensation: Applicant's agency shall compensate Provider for reasonable expenses in complying with this order.

Non-Disclosure Order: Provider shall not notify Subscriber or any other person of the existence or content of this order as follows: ☐ Until 90 days from the date of this order. ☐ Until further order of this court.

Findings

(1) Provider is an electronic communication service provider as defined in 18 USC § 2510(15) and is doing business in California.

(2) Pursuant to 18 USC §§ 2703(c)(1)(B), 2703(c), and 2703(d), this court may order a provider of an electronic communication service doing business in California to disclose the records listed above to an officer who has established reasonable grounds to believe said records are relevant and material to an ongoing criminal investigation.

(3) Applicant has filed with this court a declaration containing specific and articulable facts establishing reasonable grounds to believe the listed records are relevant and material to an ongoing criminal investigation.

(4) Applicant's declaration has established grounds for a non-disclosure order pursuant to 18 USC § 2705(b). Grounds for nondisclosure are based on the following: [check one or more]

☐ Danger to life or safety ☐ Flight from prosecution ☐ Jeopardize an investigation

☐ Evidence destruction or tampering ☐ Intimidation of potential witnesses

_____ _____

Date Judge of the Superior Court

* An application must be submitted with this order.

Recent Cases

Bobby v. Dixon

(2011) __ U.S. __ [2011 WL 5299458]

Issues

(1) Did a murder suspect effectively invoke his *Miranda* right to counsel when he refused to talk about the victim's disappearance without his attorney present? (2) After the victim's body was found, did investigators obtain the suspect's confession to the murder by employing the illegal "two step" procedure?

Facts

In order to steal Chris Hammer's car, Archie Dixon and Tom Hoffner tied him up and buried him alive. The next day, Hammer's mother reported him missing to Ohio authorities. Investigators were aware that Hammer and Dixon were acquaintances, so when a detective happened to spot Dixon at the local police station (he had gone there to recover his car which had been impounded on a traffic matter), the detective *Mirandized* him and asked if he would be willing to talk about Hammer's disappearance. Dixon said he would not talk about it without his lawyer.

In the meantime, Dixon sold Hammer's car and forged his name on the check. When investigators found out, they arrested Dixon for forgery and took him to the police station for questioning. Because of the likelihood that he would invoke his *Miranda* rights again, the officers did not seek a waiver. In any event, Dixon said he did not know anything about Hammer's disappearance. He did, however, confess to the forgery and was booked on that charge.

Later that day, Hoffner led officers to Hammer's grave, claiming that Dixon had told him that Hammer was buried there. After recovering the body, investigators brought Dixon from the jail to the police station and *Mirandized* him. This time, Dixon waived his rights and, after learning that Hammer's body had been found and that Hoffner was cooperating with the officers, he confessed to the murder. He was subsequently convicted and sentenced to death. The Sixth Circuit, however, issued a writ of habeas corpus, contending that the investigators were guilty of "grievous" *Miranda* errors. The state appealed to the United States Supreme Court which, in a *per curiam* opinon, determined that the only errors in the case were made by the Sixth Circuit.

Discussion

There were essentially two issues on appeal: (1) Did Dixon initially invoke his *Miranda* right to counsel when he refused to talk about Hammer's disappearance without his attorney present? (2) Did the investigators subsequently obtain Dixon's murder confession by employing the illegal "two step" procedure? The answer to both questions, said the Supreme Court, was no.

An invocation? The Sixth Circuit had ruled that Dixon invoked his *Miranda* right to counsel when, while visiting the police station, he refused to answer questions about Hammer's disappearance without his attorney. This ruling, said the Supreme Court, was "plainly wrong" because it is settled that a suspect can invoke his *Miranda* rights only if he was "in custody" at the time. But here, it was beyond dispute that Dixon was not in custody since he had freely gone to the police station to recover his impounded car.

Two step? As noted, when investigators questioned Dixon about forging Hammer's name on the check, they did not seek a *Miranda* waiver because they thought he would probably invoke again. Because Dixon was now in custody, his confession to the forgery was suppressed by the trial court. The propriety of the suppression order was not disputed.

The Sixth Circuit ruled, however, that this *Miranda* violation also rendered Dixon's subsequent confession to the murder inadmissible. Specifically, it held that this tactic was tantamount to the so-called "two step" procedure which the Supreme Court condemned in *Missouri* v. *Seibert*.[1] By way of background, the "two step" was a tactic in which officers would deliberately question an arrested suspect without

[1] (2004) 542 U.S. 600.

obtaining a *Miranda* waiver. Then, if he confessed or made a damaging admission, they would seek a waiver and, if he waived, they would try to get him to repeat the statement. The "two step" works on the theory that the suspect will usually waive his rights and repeat his incriminating statement because he will think (erroneously) that his first statement can be used against him and, therefore, he has nothing to lose by repeating it. That is why the Court in *Seibert* ruled that a statement obtained by means of the "two step" procedure must be suppressed.

But, as the Court pointed out in *Dixon,* there were significant differences between the questioning of Dixon and Seibert. The main difference was that, unlike Seibert, Dixon did not respond to the unwarned questioning by providing the officers with a detailed confession or otherwise "letting the cat out of the bag." In fact, Dixon claimed he didn't know anything about Hammer's disappearance. Thus, said the Court, "unlike in *Seibert*, there is no concern here that police gave Dixon *Miranda* warnings and then led him to repeat an earlier murder confession, because there was no earlier confession to repeat."

In addition, two things happened that would have caused Dixon to understand that the questioning pertaining to the murder was entirely separate from the illegal questioning that produced his confession to the forgery: (1) four hours passed between the time the investigators questioned him about the forgery and the time they questioned him about the murder, and (2) he had been informed of two major developments in the case: Hammer's body had been found, and Hoffner was cooperating with the investigators. Said the Court, "this significant break in time and dramatic change in circumstances created a new and distinct experience, ensuring that Dixon's prior, unwarned interrogation, did not undermine the effectiveness of the *Miranda* warnings he received before confessing to Hammer's murder."

Consequently, the Court ruled that the Sixth Circuit had erred when it held that Dixon's confession should have been suppressed. It added, however, that this "does not excuse the detective's decision not to give Dixon *Miranda* warnings before his first interrogation." But the appropriate remedy for this violation, said the Court, was the suppression of Dixon's confession to the forgery, and that was exactly what had occurred.

People v. Thomas

(2011) 200 Cal.App.4th 338

Issue

Under what circumstances may officers utilize a ruse to obtain a DNA sample from a suspect?

Facts

Between 2006 and 2008, several homes in Beverly Hills, Bel Air, and other affluent neighborhoods in the Los Angeles area were burglarized by a gang that became known in the media as the "Bel Air Burglars." All told, the gang stole more than $10 million worth of property and cash from the homes of, among others, Hollywood celebrities and professional athletes. At five of the crime scenes, investigators found DNA evidence, but they were unable to obtain a hit.

Then they got two breaks: a witness to one of the burglaries identified Troy Thomas as one of the burglars; and they received an anonymous tip (the crime spree had been featured on America's Most Wanted) that Thomas was involved.

While conducting surveillance on Thomas, an officer stopped him for a traffic violation. Having noticed that Thomas's eyes were bloodshot and watery, the officer asked if he would blow into a PAS device which would confirm or dispel the officer's suspicion that he was impaired. Thomas agreed and passed the test. After releasing Thomas, the officer took the PAS mouthpiece into evidence, and it was later subjected to DNA testing. The test produced a match. Detectives then obtained a warrant to search Thomas's home, and found additional incriminating evidence.

Thomas was subsequently charged with six counts of burglary. When his motion to suppress the DNA test results was denied, he pled no contest.

Discussion

Thomas urged the court to formulate three new rules that, if implemented, would have resulted in the suppression of the DNA evidence: (1) a search warrant is required to seize DNA evidence, (2) a warrant is required to test DNA evidence, and (3) officers are prohibited from using a ruse to obtain a DNA sample from a suspect.

OBTAINING A DNA SAMPLE WITHOUT A WARRANT: In response to Thomas's argument that officers should

be required to obtain a search warrant to seize DNA evidence from a suspect, the court acknowledged that a warrant would be required if a suspect were *required* to submit the sample.[2] But absent some compulsion, said the court, the acquisition of such a sample would not constitute a "search" if the suspect effectively abandoned it and had thereby surrendered any reasonable expectation of privacy in it or its evidentiary fruits. The question, then, was whether Thomas had abandoned the saliva on the PAS mouthpiece.

Although the Court of Appeal had previously ruled that a murder suspect abandoned saliva on a cigarette he discarded in a public place,[3] the situation here was somewhat different. As the court pointed out, Thomas did not intentionally discard his saliva; instead, he failed to assert a privacy interest by, for example, wiping off the mouthpiece, asking to take the mouthpiece with him, or even inquiring as to what the officer intended to do with it. In analyzing the issue, the court took note of a case in which the Supreme Judicial Court in Massachusetts ruled that a murder suspect had abandoned a saliva sample on a can of soda pop and a cigarette that detectives had given him during an interrogation. The Massachusetts court observed that "the critical act is not the making available of cigarettes and soda, if requested. Rather, it is the abandonment of the cigarette butts and soda can, and the officers promised the defendant nothing in exchange for abandonment."[4]

Based on this logic, the court ruled that Thomas had also abandoned the saliva he had deposited on the PAS device when he failed to make any effort to protect it from seizure.

WARRANTLESS TESTING: As noted, Thomas also argued that a warrant should be required to subject a person's saliva sample to DNA analysis. He reasoned that, while he might have abandoned the saliva, it could not be tested unless he knowingly consented to the testing. But the court ruled that abandoned evidence is not subject to the restrictions imposed by the Fourth Amendment, including the one that consent to search must be made knowingly.

OBTAINING DNA BY A RUSE: Finally, Thomas argued that officers should not be permitted to obtain DNA samples through "fraud and deceit." Obviously, the traffic stop and request to take a PAS test were pretexts for obtaining a DNA sample. Nevertheless, the court noted that such a ruse is permissible so long as it was not coercive and the officer had a legal right to obtain the sample. And both of these requirements were met in this case because (1) the traffic stop was lawful (Thomas did not challenge the legality of the stop), (2) there was no evidence that he was pressured into taking the PAS test, and (3) the officer did not say anything to indicate the saliva residue would not be used for some other investigative purpose.

Accordingly, the court affirmed Thomas's conviction.

People v. Nottoli

(2011) 199 Cal.App.4th 531.

Issue

Under what circumstances may officers conduct a vehicle search based on the "reasonable suspicion" standard announced in *Arizona* v. *Gant*?

Facts

At about 2 A.M. a Santa Cruz County deputy sheriff stopped a car for speeding. In the course of the stop, he observed that the driver, Reid Nottoli, was "not able to sit still"; his eyes were "watery, slightly bloodshot, and darted around in a really nervous kind of fidgeting fashion"; his speech was "rapid" and "disjointed"; he had "rapid eye tremors"; his pupils were "constricted"; and his breath was "very rapid" and "sharp."

Based on these symptoms, the deputy concluded that Nottoli was under the influence of drugs. He also learned that Nottoli was driving on an expired license. So he arrested him on both charges and confined him in his patrol car.

Having determined that it was necessary to impound Nottoli's car, the deputy conducted an inventory search during which he found a loaded .50-

[2] Citing *Skinner* v. *Railway Labor Executives' Assn.* (1989) 489 U.S. 602, 616-17 [collection of urine samples for compelled drug testing was a search].
[3] *People* v. *Gallego* (2010) 190 Cal.App.4th 388.
[4] *Comonwealth* v. *Perkins* (2008) 450 Mass. 834, 842.

caliber handgun under the driver's seat and a small amount of drugs. He also found a smart phone.

Thinking the phone might contain evidence of Nattoli's drug use or sales, the deputy pressed a key to see if it was working. The screen came to life and it showed a man wearing a mask and wielding two AR-15 assault rifles. The deputy concluded that the man was Nottoli because they were similar in size, and it appeared they were both wearing the same camouflage baseball cap. Although such rifles may be lawfully possessed by people who purchased them legally before the assault weapon ban in California, Nottoli claimed he did not own any assault rifles. Consequently, the deputy concluded that Nottoli possessed the weapons illegally, and he thought that the smart phone "would have evidence of possibly gun-related crimes, such as discussions related to obtaining, trafficking or selling illegal weaponry," and that it might also "contain further evidence of drug use, drug transactions, and drug trafficking."

At this point, the deputy handed the phone to another deputy who searched it and found, among other things, an email receipt from an internet gun broker for the purchase of "incendiary projectiles" for a .50-caliber handgun.

A chemical test later showed that Nottoli was not under the influence stimulants, although he tested "presumptive positive" for marijuana and opiates. He was subsequently charged with, among other things, possession of an assault weapon. (Nottoli died eight months later while this case was pending. Although this rendered the case moot, the court issued its opinion "because it raises important issues of public interest that are likely to recur in other cases.")

Discussion

The central issue on appeal was the legality of the cell phone search. At the outset, the court rejected the argument that the search qualified as an inventory search. This was because the law is settled that, even when officers have a legal right to conduct an inventory search, they may search only those places and things they were permitted or required to search pursuant to standard departmental policy or standard procedure.[5] But no testimony was presented that the search of the cell phone was conducted in accordance with such a policy or procedure.

The People also argued that the search qualified as a search incident to arrest as defined by the United States Supreme Court in *Arizona* v. *Gant*.[6] In *Gant*, the Court ruled that officers who have made a custodial arrest of an occupant of a vehicle may search the passenger compartment if either of the following circumstances existed:

(1) **ARRESTEE HAD ACCESS**: The arrestee had immediate access to the passenger compartment when the search occurred.

(2) **REASONABLE SUSPICION**: Officers reasonably believed they would find evidence in the passenger compartment pertaining to the crime for which the occupant had been arrested.

It was apparent that the first exception did not apply because Nottoli had been handcuffed and confined in a patrol car when the search occurred. Thus, the issue was whether the second exception applied. And in deciding this issue, the court had to answer the following question: To conduct such a search, must officers be aware of specific facts that support a reasonable belief that evidence of the alleged crime will be found in the vehicle? Or, is it enough that they knew that the people who commit such a crime often possess fruits or instrumentalities? For example, if officers arrest the driver of a car for DUI, do they automatically have reasonable suspicion to search for liquor, or must they also be able to testify as to the existence of specific circumstances that reasonably indicate there is liquor inside?

The court in *Nottoli* ruled that specific facts are not required, that the propriety of the search depends solely on the nature of the crime for which the person was arrested. Accordingly, because the deputy had probable cause to arrest Nottoli for being under the influence of drugs, he could search the vehicle for

[5] See *Florida* v. *Wells* (1990) 495 U.S. 1, 4 [search must be conducted in accordance with "standardized criteria or established routine"]; *Colorado* v. *Bertine* (1987) 479 U.S. 367, 374, fn.6 ["Our decisions have always adhered to the requirement that inventories be conducted according to standardized criteria."].

[6] (2009) 556 U.S. 332.

evidence pertaining to the crime. Said the court, the arrest itself "supplied a reasonable basis for believing that evidence relevant to that type of offense might be in his vehicle."

Having determined that the search of the passenger compartment was lawful, the court had to decide whether the officers were also permitted to search the cell phone. Here, the court ruled that when officers have a legal right to search the passenger compartment of a vehicle based on reasonable suspicion, they are not required to limit the search to places and things in which relevant evidence might be found. This ruling was based on the court's reading of *Gant*, and its conclusion that *Gant* "does not require any degree of probability that evidence bearing on that offense will be found in a particular container that is searched."

The court also ruled, however, that even if such searches must be restricted to places and things in which relevant evidence might reasonably be found, the search of the cell phone would have been lawful because the deputy testified that, "in his experience, drug users and sellers use cell phones as their main communication and cell phones can contain text messages related to acquiring and offering drugs."

For these reasons, the court ruled that the search of Nottoli's cell phone was lawful and, therefore, "the deputies had unqualified authority under *Gant* to search the passenger compartment of the vehicle and any container found therein, including [Nottoli's] cell phone."

Comment

After *Nottoli* was decided, another appellate court in California addressed a similar issue. In *People* v. *Evans*,[7] LAPD gang enforcement officers stopped a car for failing to signal a turn. One of the officers asked the driver, Evans, to exit the car, but instead he kept asking why he had been stopped. Although the officer explained the reason, Evans kept repeating the question and saying he wanted to talk with the officer's supervisor. This went on for about ten minutes, after which officers broke a window, tased Evans, and arrested him for interfering with an investigation in violation of Penal Code § 148. Officers subsequently searched the car and found rock cocaine hidden in an air vent.

As in *Nottoli*, the search could not be upheld as an inventory search because there was no evidence that it was conducted pursuant to standard criteria. But unlike *Nottoli*, the search could not be based on reasonable suspicion because, as the court pointed out, "[i]mpeding an officer's investigation is unlikely to leave evidentiary traces, such as the fruits or instrumentalities of the crime, in a vehicle."

Two other things about these types of searches should be noted. First, they will be permitted only if the sought-after evidence pertains to the same crime for which the occupant was arrested. For example, the officers who arrested Evans apparently also had reasonable suspicion to believe he possessed drugs. But because he was not arrested for a drug offense, the search could not be based on that ground.

Second, because officers must have *reasonably* believed they may find fruits or instrumentalities of the alleged crime in the passenger compartment, wild speculation will be disregarded. For example, if the driver was arrested for driving on a suspended license with knowledge of the suspension, it is conceivable that relevant evidence consisting of a DMV suspension-notification letter would be found in the vehicle. But it is doubtful that such a weak connection between the crime and the evidence would constitute justification for a search.[8]

Robey v. Superior Court

(2011) 200 Cal.App.4th 1

Issue

If officers lawfully possess a container belonging to a suspect, and if they have probable cause to believe it contains drugs, are they required to obtain a warrant before searching it?

Facts

Police in Santa Maria received a call from an employee at a local FedEx office who said she could smell the odor of marijuana coming from a package that Kewhan Robey had dropped off for delivery. When officers arrived, they confirmed that the odor

[7] (2011) __ Cal.App.4th __ [2011 WL 5252792].

[8] See *Arizona* v. *Gant* (2009) 556 U.S. 332, __ [arrest for driving on a suspended license was "an offense for which police could not expect to find evidence in the passenger compartment"].

emanating from the package was, in fact, that of marijuana. They did not, however, search the package there; instead, they took it to the police station where they opened it and found approximately 15 ounces of marijuana. After Robey was arrested and his motion to suppress the marijuana was denied, he appealed.

Discussion

Robey contended that the search of his package was illegal because the officers did not obtain a warrant. Although the Court of Appeal acknowledged that the officers had probable cause to believe that the package contained marijuana, and although it ruled that they had a legal right to search it at the FedEx office, it held that the search was illegal because it occurred at the police station. Citing the California Supreme Court's decision in *People* v. *McKinnon,*[9] the court said, "Once [the officers] elected to seize the package, *McKinnon* did require that the police officers hold the package until they obtained a search warrant."

The court also rejected the People's argument that the search was lawful under the "plain smell" variant of the "plain view" doctrine. Under the "plain view" rule, an intrusion into a container in an officer's lawful possession does not constitute a "search" under the Fourth Amendment if the officer had probable cause to believe there were drugs or other evidence of a crime inside. But the court, based on its interpretation of another California Supreme Court opinion, ruled that there is a difference—of constitutional magnitude—between probable cause based on plain smell and probable cause based on other factors; and that plain smell alone is insufficient to justify a warrantless search of a container.

For these reasons, the court ruled the search of Robey's package was illegal, and the marijuana should have been suppressed.

Comment

There are several problems with the court's reasoning. First, it is apparent that the officers' act of opening Robey's package did not constitute a "search" under the Fourth Amendment—and thus a search warrant was not required—because its contents were self-evident. As the United States Supreme Court explained, "[A] Fourth Amendment search does not occur . . . unless the individual manifested a subjective expectation of privacy in the object of the challenged search, and society is willing to recognize that expectation as reasonable."[10] But Robey could not have reasonably expected that the contents of his package would remain private because (1) the contents consisted of an illegal substance that has a notoriously distinct and unusual odor,[11] and (2) he did not take adequate measures to prevent this odor from escaping from the package.

In fact, in another odor-of-marijuana-in-a-container case, the California Supreme Court expressly rejected the reasoning employed in *Robey*. The case was *People* v. *Mayberry*[12] and, although *Robey* did not even cite it, the following passage seems pertinent:

> In our view, the escaping smell of contraband from luggage may be likened to the emanation of a fluid leaking from a container. The odor is detectable by the nose, as the leak is visible to the eye. We discern no constitutionally significant difference in the manner of escape, and conclude that any privacy right is lost when either escapes into the surrounding area.

Strangely, the *Robey* court seemed perplexed as to whether the odor of marijuana can generate probable cause. At one point it said Robey's package "reeked of marijuana" and elsewhere it said the odor of marijuana "gave the officers probable cause to obtain a search warrant." But elsewhere, it claimed that marijuana has only an "alleged pungent odor," and that to smell marijuana "is not the same as to see it."

---

[9] (1972) 7 Cal.3d 899.

[10] *Kyllo* v. *United States* (2001) 533 U.S. 27, 33. Also see *Minnesota* v. *Dickerson* (1993) 508 U.S. 366, 375 ["The rationale of the plain-view doctrine is that if contraband is left in open view and is observed by a police officer from a lawful vantage point, there has been no invasion of a legitimate expectation of privacy and thus no 'search'"]; *Illinois* v. *Andreas* (1983) 463 U.S. 765, 771 ["The plain view doctrine is grounded on the proposition that once police are lawfully in a position to observe an item first-hand, its owner's privacy interest in that item is lost."].

[11] See *People* v. *Benjamin* (1999) 77 Cal.App.4th 264, 273 ["Odors may constitute probable cause if the magistrate finds the affiant qualified to know the odor, and it is one sufficiently distinctive to identify a forbidden substance."].

[12] (1982) 31 Cal.3d 335, 342.

It is noteworthy that while the *Robey* court believes that marijuana has only an "*alleged*" pungent odor, the justices of the United States Supreme Court have stated without qualification that it has a "distinct" odor.[13] (This seems to undermine the suspicion that the justices of the Supreme Court live sheltered lives. But it raises questions about certain justices of the Court of Appeal.)

Second, the court's bold announcement that there is a difference of constitutional magnitude between probable cause based on plain smell and probable cause based on plain view or other circumstances is groundless, which probably explains the court's failure to provide an analysis of the issue. In reality, probable cause is probable cause—regardless of the circumstances upon which it was based. This was settled almost 30 years ago when the United States Supreme Court ruled in *Illinois* v. *Gates* that if officers are aware of a fact or facts that demonstrate a "fair probability" that something contains contraband or other evidence of a crime, they have probable cause—and no further discussion is necessary.[14] Similarly, in his concurring opinion in *Guidi* v. *Superior Court*, Justice Mosk explained that "the sense of smell, and indeed all the senses, may be employed, not merely in confirmation of what is already visible, but in equal weight with the sense of sight in the determination of probable cause to search."[15]

Third, the court in *Robey* represented that its ruling was mandated by the California Supreme Court's decision in *People* v. *McKinnon* (cited earlier), a case which also involved the search of a marijuana-filled package that was discovered by a common carrier. Here is what the *Robey* court said:

> The court [in *McKinnon*] held that when the police have probable cause to believe that a package consigned to a common carrier contains contraband, they are entitled either to search it immediately without a warrant or to seize and hold it until they can obtain a warrant.

Note the word "immediately." It was this word that, according to the *Robey* court, rendered the search of Robey's package illegal because the search did not occur immediately at the FedEx office. But the court in *McKinnon* did not say the search must occur "immediately." In fact, the *McKinnon* court did not place any temporal restrictions on when the search must occur. Here is what the court actually said:

> [W]hen the police have probable cause to believe a chattel consigned to a common carrier contains contraband, they must be entitled either (1) to search it without a warrant or (2) to "seize" and hold it until they can obtain a warrant . . .

Elsewhere, the court said:

> [W]e conclude that . . . a chattel consigned to a common carrier for shipment may lawfully be searched upon probable cause to believe it contains contraband.[16]

While it is true that the search in *McKinnon* occurred at the carrier's office, as the above passages demonstrate, the court did not rule this was a requirement. And that is not surprising because the intrusiveness of the search of a package does not depend one iota on whether it occurred where it was found or whether it occurred later at another location. As the United States Supreme Court observed, "[R]equiring police to obtain a warrant once they have obtained a first-hand perception of contraband, stolen property or incriminating evidence generally would be a needless inconvenience."[17]

Finally, the court ruled that although the officers were entitled to seize the package, they were not allowed to search it without a warrant. It is, however, unthinkable that officers would be expected to take possession of a container and transport it to a police station or some other location without knowing whether it also contained something that might harm them. As the California Supreme Court explained, "[T]he power to seize carries with it the power to 'search' the seized item."[18]

[On November 4, 2011, the Santa Barbara County DA's Office petitioned the California Supreme Court to review the *Robey* decision. The California Attorney General's Office will be filing an amicus brief.]

---

[13] *United States* v. *Johns* (1985) 469 U.S. 778, 482. Also see *People* v. *Gale* (1973) 9 Cal.3d 788, 794 ["the strong odor of fresh marijuana which [the officer] smelled after entering [the vehicle] would have given him probable cause to believe that contraband may be present"].

[14] (1983) 462 U.S. 213, 237.

[15] (1973) 10 Cal.3d 1, 20 [conc. opn. of Mosk, J.].

[16] (1972) 7 Cal.3d 899, 902-903.

[17] *Texas* v. *Brown* (1983) 460 U.S. 730, 739.

[18] *Guidi* v. *Superior Court* (1973) 10 Cal.3d 1 17.

People v. Nelson

(2011) __ Cal.App.4th __ [2011 WL 5515547]

Issue

Does a driver violate Vehicle Code section 23123 if he uses a cell phone while stopped at a traffic signal?

Facts

While waiting at a stop light in Richmond, Carl Nelson dialed a number on his cell phone and held the phone up to his ear. Unbeknownst to him, a Richmond motorcycle officer had stopped next to him and saw the whole thing. When Nelson realized that the officer was watching him, he put the phone away, but it was too late: When the light turned green, the officer stopped him.

Nelson tried to convince the officer that he did not violate the cell phone prohibition because his car was not actually moving when he used the phone and, thus, he was not technically "driving" his car at the time. The officer was unconvinced; he wrote him a ticket and Nelson contested it in traffic court. He lost, and although he also lost his appeal to the Superior Court in Contra Costa County, the court certified the matter to the Court of Appeal for review.

Discussion

Vehicle Code section 23123 states: "A person shall not drive a motor vehicle while using a wireless telephone unless that telephone is specifically designed and configured to allow hands-free listening and talking, and is used in that manner while driving." As noted, Nelson argued that he did not violate the statute because he was not "driving" his vehicle at the time. He pointed out that a contrary conclusion would lead to absurd results, such as a driver being cited if he used a cell phone while at a dead stop for hours because of a serious traffic accident up ahead.

While such a situation would constitute a technical violation, the court noted that it was ruling only on whether Nelson violated the statute—and it ruled that he did. As the court pointed out, if it adopted Nelson's interpretation "we would open the door to millions of people across our state repeatedly picking up their phones and devices to place phone calls and check voicemail (or text-based messages) every day while driving whenever they are paused momentarily in traffic, their car in gear and held still only by their foot on the brake, however short the pause in the vehicle's movement. This could include fleeting pauses in stop-and-go traffic, at traffic lights and stop signs, as pedestrians cross, as vehicles ahead navigate around a double-parked vehicle, and many other circumstances."

In a concurring opinion, Justice Richman explained that he agreed with the ruling, but for the following reason: "A shopper driving to a store near Lake Merritt in Oakland may have to stop while a gaggle of geese crosses the street. A couple going for a Sunday drive in West Marin County may have to stop for a cattle crossing. And, of course, all of us are expected to stop for red lights, stop signs, crossing trains, and funeral processions. In short, all drivers may, and sometimes must, stop. But they do so while 'driving. Just like defendant."

Update: "Open carry"

On January 1, 2012, a law went into effect that bans the open carrying of unloaded handguns in California. Although there are certain exceptions, the law generally makes it a misdemeanor to carry an exposed and unloaded gun in a public place. The law has been codified as Penal Code section 26350 *et sec.*

Update: DNA collection from arrestees

On October 19, 2011, the California Supreme Court announced it would review the case of *People* v. *Buza*[19] in which the Court of Appeal ruled that Pen. Code section 296 is unconstitutional as to its provision authorizing the taking of DNA samples from arrestees without a warrant. As the result of the Supreme Court's action, *Buza* was depublished.

Update: Searching cell phones

As we reported in the Spring 2011 edition, the California Supreme Court ruled in *People* v. *Diaz*[20] that officers who have made a custodial arrest of a person may, as an incident to the arrest, search a cell phone in his possession. On October 3, 2011, the U.S. Supreme Court denied a petition by Diaz to review the California Supreme Court's decision. POV

[19] (2011) 197 Cal.App.4th 1541.
[20] (2011) 51 Cal4th 84

The Changing Times

Alameda County District Attorney's Office

Capt. **Lisa Foster**, who was director of the Victim Witness Division, retired after 34 years in law enforcement. Lisa began her career in 1977 when she joined the Los Angeles County Sheriff's Department. She became an Oakland police officer in 1981, and joined the DA's Office in 1989. Lt. **Cindy Hall** retired after 21 years in the DA's Office and eight years at Oakland PD. New inspectors: **Andre Rachal** (from Oakland PD), and **Andrea Moreland** (from the Contra Costa County DA's Office).

On December 2nd, former U.S. Attorney General **Ed Meese** returned to the District Attorney's Office at the Alameda County Courthouse where he began his legal career 53 years ago. The occasion was a surprise party for Ed's 80th birthday; and it was well attended by, among others, federal and state judges and former DA's who worked with him.

Alameda County Narcotics Task Force

Transferring out: **Dave Greaney** (East Bay Regional Parks PD), **Bruce Calero** (CHP), **Mike Pozner** (Probation Dept.), **Shawn Peterson** (ACSO), and **Ben Beltramo** (DA's Office). Transferring in: **Gary Castenada** (East Bay Regional Parks PD), **Dalen Randa** (Probation Dept.), **Miguel Ibarra** (ACSO), and **George Wood** (DA's Office).

Alameda County Sheriff's Office

The following deputies have retired: Sgt. **Dwaine Montes** (24 years), **Harry Wynn** (31 years), **Daniel Lonergan** (23 years), and **Denny Adams** (22 years).

Alameda Police Department

Capt. **Jim Brock** retired after 30 years of service. **Gary Self** and **David Ellis** retired after a total of 30 years, both started at Oakland PD and finished with 16 years at Alameda PD. **Judy Pena** retired after 10 years of service. Dispatcher **Kathryn Boyd-Fernandez** retired after 34 years of service. **David Pascoe** was promoted to acting sergeant.

Transfers: Sgt. **Eileen Tannahill** from Patrol to Property Crimes Investigations, Sgt. **Wayland Gee** from Property Crimes to Violent Crimes Investigations, **Rod Rummel** from Patrol to Personnel and Training, **Mike Ortega** from Patrol to Special Investigations, **Emilia Mrak** from Patrol to Community Oriented Policing Preventative Services, **Rob Heckman** from Special Investigations to Patrol, **Ryan Derespini** and **Matt McMullen** from Patrol to Violent Crimes Investigations. **David Lloyd** and **Brian Foster** were selected as new K-9 handlers.

Berkeley Police Department

The following officers have retired: Capt. **Dennis Ahearn** (31 years), **John Nutterfield** (17 years), and **Steve White** (21 years). **Doug Golden** accepted a position with the police department in Alexandria, VA. Former Berkeley PD trainee **Lee E. Martin, Jr.** retired from the CHP (West L.A. office) after 31 years of service. Lateral appointment: **Jamie Lucero**. Recruits **Jason Muniz** and **Andres Bejarano** are attending the Santa Clara Police Academy. The department reports that retired sergeants **Michael Reppas** and **Michael Stafstrom** have passed away. **Michael Reppas** served BPD from 1950-1979, and **Michael Stafstrom** served from 1971-2002.

California Highway Patrol

Dublin office: Lt. **Zachary Johnson** was promoted to captain and was appointed commander of the Dublin CHP office.

East Bay Regional Parks Police Dept.

Academy graduate **James Michalosky** was hired as a police officer. **Anthony Dutra** and **Ryland Macfadyen** were hired as police recruits.

Emeryville Police Department

PST **Yesenia Arevalo** has joined Arcata PD. She had been with Emeryville PD for seven years. PST **Connie Johnson**, the department's property and evidence clerk is also the department chaplain and one of EPD's crisis negotiators, and is a member of the Alameda County Emergency Manager's Association and represents EPD as a tactical dispatcher. She recently gave an informative presentation to the association on Critical Incident Stress Management,

speaking on the importance of managing stress in our personal and work lives, and how to recognize key indicators that might lead to health issues. Her presentation was very well received and EPD is very proud of her accomplishments.

FREMONT POLICE DEPARTMENT

Lateral appointments: **Paul Soper** (San Jose PD), **Cameron Newton** (San Jose PD), and **Jennifer Allsup** (Alameda County SO). New officers: **Brian Fuellenbach** and **Brian Holscher**. New communication dispatchers: **Angel Lee**, **Juliana Cruz**, and **Chrystal Leinweber**. New detention officer: **Kenneth Harrison**.

NEWARK POLICE DEPARTMENT

Sgt. **Renny Lawson** was promoted to commander. **Chomnan Loth** was promoted to sergeant. **Sam Ackerman** transferred from Patrol to Detectives. **Nick Mavrakis** transferred from Patrol to K9 along with his partner "**Ares**." **Pat Smith** and his partner "**Henk**" completed seven years of service in the K9 detail; Pat returned to Patrol.

OAKLAND HOUSING AUTHORITY POLICE DEPT.

Lt. **James Williams** was appointed Interim Chief of Police. **Vic Li** and **Derek Souza** transferred from Patrol to Investigations.

OAKLAND POLICE DEPARTMENT

Chief of Police **Anthony Batts** resigned after two years of service and has taken a position at Harvard University where he will conduct research and work on executive policymaking in police departments. Chief Batts was formerly chief of the Long Beach PD. Assistant Chief **Howard Jordan** was named Interim Chief of Police.

Andre Rachal retired after 25 years of service. The following officers left OPD to join other agencies: **Kittrell Carter** (Alameda PD), **Scott Bezner** (Walnut Creek PD), **Kyle Petersen** (Sonoma County SO), **Steven Szopinski** (BART PD), and **Michael Spediacci** (Santa Rosa PD). The following officers have taken disability retirements: Sgt. **Rayomond Sethna**, Sgt. **Todd Crutchfield**, Sgt. **Craig Hardison**, **Anthony Burns**, **Michael Healy**, and **Donald Koch**.

The department reports that the following retired officers have died: **Palmer Stinson** (retired in 1974), **Robert B. Wilson** (retired in 1981), **Charles H. Wood, Jr.** (retired in 1976), **Larry D. Howerton** (retired in 1981), **Gordon Miller** (retired in 1977), and **Alner Brewer** (retired in 1999).

PLEASANTON POLICE DEPARTMENT

Ted Young and **Julie Fragomeli** were promoted to sergeant and transferred to the Operations Division.

SAN LEANDRO POLICE DEPARTMENT

Capt. **Pete Ballew** retired from the department after 27 years of service. **Joe Molettieri** was promoted to sergeant and assigned to the Patrol Division. Lt. **Jeff Tudor** graduated from the National Academy in December 2011. Sgt. **Doug Calcagno** graduated from the Los Angeles Police Department Leadership Academy in December 2011.

Transfers: Sgt. **Mike Sobek** from Criminal Investigation Division to Patrol Division, Sgt. **Troy Young** from Patrol Division to Administrative Patrol Sergeant, **Josh Brum** from Patrol Division to Criminal Investigation-Crimes Against Persons, **Ali Khan** from Patrol Division to Criminal Investigation-Special Victims Unit, **Robert Mendenhall** from Patrol Division to Traffic Division, **Matt Barajas** from Patrol Division to Criminal Investigation-Vice/Narcotics, **Brian Buss** will be assigned to the Bicycle Unit, **Neil Goodman** from Criminal Investigation Division to Patrol Division, **Alex Rendez** will be assigned to the Patrol Division.

The department is sad to report that retired officer **Floyd Pierini** passed away at the age of 83 on November 23, 2011. He worked for the department as an officer and detective from 1956 – 1979.

UNIVERSITY OF CALIFORNIA, BERKELEY POLICE DEPARTMENT

Newly appointed officers: **Stephanie Martinez**, **Cameron Soo**, and **Roderick Roe**. POV

War Stories

A mom with clout

At Marshalls department store in Fremont, a loss prevention officer arrested a 16-year old boy for shoplifting. But when he phoned the boy's mother to pick him up, she refused, saying she wanted him sent to juvenile hall because he needed to be taught a lesson. So the officer phoned Fremont police. When an officer arrived, the boy told him that he *wanted* to go to juvenile hall because he was afraid of what his mother would do to him when she found out he had been arrested. But the officer explained that juvenile hall wouldn't take him because his crime, shoplifting, was too minor. "That's not a problem," said the boy, "'cause I've done more stuff than shoplifting." At that point, he started giving the details of his many other criminal pursuits, including a certain residential burglary and an attempted robbery, both of which were under investigation by FPD at the time. Needless to say, the boy got his wish.

That's good advice

A man who was caught shoplifting in a Long's Drug store in Hayward had a seizure while waiting in the security office. He was transported by ambulance to the emergency department at Eden Medical Center where he was treated for an adverse heroin reaction. As he was being released to the custody of an officer, the doctor handed the man a document headed "AFTERCARE INSTRUCTIONS." In the section marked "You can do the following to help you feel better," the doctor had written, "Don't shoplift."

Thinking ahead

A man who bailed out of stolen car and ran from CHP officers in Hayward was arrested a few minutes later in a nearby Jack-in-the-Box as he sat eating a cheeseburger. When one of the officers asked him why he'd gone into the restaurant, he replied, "Well, I saw you guys driving around looking for me. And you were probably gonna catch me. So I went inside for a burger and some fries. I figured this would be my last chance for a while."

A wonderful witness

In a Los Angeles courtroom, the defendant's attorney was cross-examining a prosecution witness who had just identified the defendant as the man who shot and killed a security guard during a takeover robbery at a marijuana clinic:

Attorney: You have said that it's your *belief* that my client was . . .

Witness [interrupting]: No counselor, it's not my *belief*. I *know* he pointed a gun at the guard's head and shot him! That guy right there! That's him! I'm positive! [The defendant was convicted.]

The unhappy tale of the man who stole a motor officer's sunglasses

Oakland police motorcycle officer Eddy Bermudez stopped a driver on International Blvd., put his Oakley sunglasses on top of the gas tank, and walked up to the car. Just then, a passing motorist yelled at him, "Hey, that guy just stole your sunglasses!" The motorist was pointing to a man who had just walked into a bar, so the officer confronted the man, who confessed and returned the sunglasses. The officer then arrested him for petty theft and, during a search incident to arrest, found a load of methamphetamine and paraphernalia. Said the officer, "How crazy is that!"

Finders keepers

A man notified Albany police that a suspicious backpack had been abandoned at the bottom of a stairwell in an apartment building. The responding officer located the backpack, which reeked of marijuana. So he opened it and found lots of marijuana packakaged for sale and a digital scale. Just then, a young man walked down the stairwell and yelled, "Hey, that's my backpack!" The officer replied, "Well, that's sure a coincidence. I was just thinking how much I'd like to meet the guy who owned this." After the officer arrested and *Mirandized* him, the man admitted that he had been in the business of selling marijuana at Berkeley City College.

A whopper

A Hayward police officer obtained consent to search a suspected drug dealer. As the officer extracted a large bindle of methamphetamine from the suspect's pants pocket, the suspect exclaimed, "That's not mine, man. Those aren't even my pants."

A bigger whopper

While searching a man incident to arrest, an officer in Union City found a methamphetermine smoking pipe. "That's not mine," said the man. The officer decided to bluff him, saying "I don't believe you, so I'm going test that pipe to see if your DNA is on it." The man thought for a second, then said,"Well, my DNA might be on it, but that's because some dude put the pipe on my lips while I was sleeping without my knowledge and then put it in my pocket."

Never mind

The Alameda County Sheriff's Office received a 911 call that a man was trying to murder another man by drowning him in a mud pit in a ravine in Sunol. When deputies arrived, they found two men in the pit—both covered in mud. But it turned out there was no crime. The men explained that they were just taking a mud bath.

How the law works in Kentucky

In granting a motion to settle a case in Kentucky, the court issued the following decree: "Such news of an amicable settlement made this Court happier than a tick on a fat dog because it is otherwise busier than a one legged cat in a sand box."

Police work can be fun

One afternoon in San Leandro, a truck driver was blocking two lanes of traffic as he tried to make an illegal U-turn. When the motorists behind him started honking their horns and yelling, the truck driver lost it—jumping out of his truck, running from car to car, and swearing at the drivers. When he got to the last car in the line, he screamed "What the fuck do you want?" Without waiting for an answer, he went back in his truck and drove off. It happened that the last car in line was an unmarked San Leandro police car, and the officer who was driving it promptly pulled in behind the truck and lit it up. As the driver rolled down his window, the officer said, "Remember me? You asked me what I wanted. Let's start with your driver's license, registration, and proof of insurance."

Take two

One afternoon in Florida, a rookie bank robber burst into a bank, pulled out a handgun and yelled, "Freeze, mother-stickers! This is a fuck up!" For a moment, everyone was silent. Then some of the tellers and customers started giggling, which developed in chuckling, then sidesplitting laughter. The robber was so embarrassed he turned around and ran away.

How romantic

The following ad appeared in the "Personals" section of a newspaper in San Francisco:

> San Francisco Hall of Justice. Early morning. You going in handcuffed with a black eye. Me coming out. You smiled. I shrugged. Let's have a drink.

Let's have a War Story, too!

The War Story Hotline

Email: POV@acgov.org
Mail: 1225 Fallon St., Room 900
Oakland, CA 94612

Now Shipping!

The 16th Annual Edition of California Criminal Investigation

Revised and Updated

For details or to order online
www.le.alcoda.org