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.