Governmental Tracking of Cell Phones and Vehicles: The Confluence of Privacy, Technology, and Law

Richard M. Thompson
Law Clerk

December 1, 2011

Congressional Research Service
7-5700
www.crs.gov
R42109

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

Technology has advanced considerably since the framers established the constitutional parameters for searches and seizures in the Fourth Amendment. What were ink quills and parchment are now cell phones and the Internet. It is undeniable that these advances in technology threaten to diminish privacy. Law enforcement's use of cell phones and GPS devices to track an individual's movements brings into sharp relief the challenge of reconciling technology, privacy, and law.

Beyond the Constitution, a miscellany of statutes and cases may apply to these tracking activities. One such statute is the Electronic Communications Privacy Act of 1986 (ECPA), P.L. 99-508, 100 Stat. 1848 (1986), which protects individual privacy and governs the methods by which law enforcement may retrieve electronic communications information for investigative purposes, including pen registers, trap and trace devices, wiretaps, and tracking devices. The primary debate surrounding cell phone and GPS tracking is not whether they are permitted by statute but rather what legal standard should apply: probable cause, reasonable suspicion, or something less.

Legislation has been introduced in the 112th Congress that proposes to update, clarify, or, in some instances, strengthen the privacy interests protected under the law and give law enforcement a clearer framework for obtaining crucial crime-fighting information. In particular, Senator Ron Wyden and Representative Jason Chaffetz introduced identical legislation, S. 1212 and H.R. 2168, entitled the Geolocational Privacy and Surveillance Act, or GPS bill, which would make it unlawful for a service provider to disclose or law enforcement to intercept or use a person's location unless they obtained a warrant based upon probable cause or one of the limited exceptions applies. Senator Patrick J. Leahy has introduced the Electronic Communications Privacy Act Amendment Act of 2011 (S. 1011), which not only includes a warrant requirement for geolocation information, but also overhauls and updates other provisions of federal electronic surveillance law.

Congress is not the only branch confronting this tension between technology and privacy—the Supreme Court has granted certiorari in *United States v. Jones*, 131 S. Ct. 3064 (2011), to determine whether the Fourth Amendment's protection against unreasonable searches and seizures precludes the police from placing a GPS device on a person's vehicle without a warrant. Though the Court has dealt with similar issues in *United States v. Knotts*, 460 U.S. 276 (1983), and *United States v. Karo*, 468 U.S. 705 (1984), in *Jones*, the Court has been asked to determine what effect the prolonged, warrantless use of a tracking device has on a person's privacy interest.

This report will briefly survey Fourth Amendment law as it pertains to the government's tracking programs. It will then summarize federal electronic surveillance statutes and the case law surrounding cell phone location tracking. Next, the report will describe the GPS-vehicle tracking cases and review the pending Supreme Court GPS tracking case, *United States v. Jones*. Finally, the report will summarize the geolocation and electronic surveillance legislation introduced in the 112th Congress.

Contents

Contacts

Introduction

Technology has advanced considerably since the framers established the constitutional parameters for searches and seizures in the Fourth Amendment. What were ink quills and parchment are now cell phones and the Internet. It is undeniable that these advances in technology threaten to diminish privacy. Law enforcement's use of cell phones and GPS devices to track an individual's movements brings into sharp relief the challenge of reconciling technology, privacy, and law.

A miscellany of statutes and cases may apply to these tracking programs. One such statute is the Electronic Communications Privacy Act of 1986 (ECPA),[1] which protects individual privacy and governs the methods by which law enforcement may retrieve electronic communications for investigative purposes. ECPA addresses various means for conducting these investigations, including pen registers, trap and trace devices, wiretaps, and tracking devices. The primary debate surrounding statutory regulation of cell phone and GPS tracking is not whether they are permitted, but rather what legal standard should apply: probable cause, reasonable suspicion, or something less. More fundamentally, the Constitution sets a floor for permissible tracking practices.

Legislation has been introduced in the 112th Congress that proposes to update, clarify, or, in some instances, strengthen the privacy interests protected under the law and give law enforcement a clearer framework for obtaining crucial crime-fighting information. In particular, Senator Ron Wyden and Representative Jason Chaffetz introduced identical legislation, S. 1212 and H.R. 2168, the Geolocational Privacy and Surveillance Act (GPS bill), which would make it unlawful for a service provider to disclose a person's location unless law enforcement obtained a warrant based upon probable cause or one of the limited exceptions applies. Senator Al Franken has introduced the Location Privacy and Protection Act of 2011 (S. 1223)—similar to the GPS bill, but which applies only to private, not governmental, actors. Senator Patrick J. Leahy has introduced the Electronic Communications Privacy Act Amendment Act of 2011 (S. 1011), which not only includes a warrant requirement for geolocation information, but also overhauls and updates other provisions of federal electronic surveillance law.

Congress is not the only branch confronting this tension between technology and privacy—the Supreme Court has granted certiorari in *United States v. Jones*, to determine whether the Fourth Amendment's protection against unreasonable searches and seizures precludes the police from placing a GPS device on a person's vehicle without a warrant.[2] Though the Court has dealt with similar issues in *United States v. Knotts*,[3] and *United States v. Karo*,[4] in *Jones*, the Court has been asked to determine what effect the prolonged, warrantless use of a tracking device has on a person's privacy interest.

The use of geolocation information by private actors (e.g., telecommunication companies, commercial service providers) also raises significant privacy concerns.[5] As more computing

[1] Electronic Communications Privacy Act of 1986, P.L. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

[2] United States v. Maynard, 615 F.3d 544, 555-56 (D.C. Cir. 2010), *cert. granted sub nom.* United States v. Jones, 131 S. Ct. 3064 (2011) (No. 10-1259) (oral arguments held on November 8, 2011).

[3] United States v. Knotts, 460 U.S. 276 (1983).

[4] United States v. Karo, 468 U.S. 705 (1984).

[5] *See* CRS Report R41756, *Privacy Protections for Personal Information Online*, by Gina Stevens.

moves to the "cloud," concerns are raised as to what privacy protections consumers should be accorded. The proposed legislation from the 112th Congress just described applies to both government and private actors, and attempts to address some of these issues. However, an analysis of the private use of this type of information is beyond the scope of this report.

This report will briefly survey Fourth Amendment law as it pertains to the government's tracking programs. It will then summarize federal electronic surveillance statutes and the case law surrounding cell phone location tracking. Next, the report will describe the GPS-vehicle tracking cases and review the Supreme Court GPS tracking case, *United States v. Jones*. Finally, the report will summarize the geolocation and electronic surveillance legislation introduced in the 112th Congress.

Fourth Amendment and Privacy

The fountainhead of privacy in the United States is the Fourth Amendment, which ensures that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated...."[6] For at least the past 50 years, this provision has been subject to more litigation than any other in the Bill of Rights.[7] This may come as no surprise, considering the Fourth Amendment protects, as Justice Brandeis put it, "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[8]

A recurrent theme flows through Fourth Amendment cases: criminals devise new ways to commit crimes and evade the police; the police devise new ways to intercept communications and detect criminal conduct; and the courts are left to sort out the constitutional from the not in these new contexts. In 1928, for example, when police eavesdropped on the telephone conversations of Roy Olmstead and his bootlegging conspirators, the Court refused to label this a violation of the Constitution because the police had not physically trespassed on the defendants' properties in making the wiretaps.[9] The Fourth Amendment protected a person's property interest, the Court held, not abstract things like his own voice.[10] Also, the channel of communication, the telephone wires, extended beyond the defendant's home to the "whole world"—well beyond Olmstead's property interest.[11]

Almost 40 years later the Court changed course, radically altering the constitutional contours of protected privacy by determining that "the Fourth Amendment protects people, not places."[12] In *Katz v. United States*, the FBI eavesdropped on Katz's conversation with an electronic device after he had closed himself inside of a telephone booth. The Court found that act of closing himself in a booth indicated Katz's desire for privacy, and that the FBI had overstepped its

[6] U.S. CONST. amend. IV.

[7] 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT IX (4th ed. 2004).

[8] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); *see generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). For a general overview of privacy law, see Stevens, *supra* note 5.

[9] *Olmstead*, 277 U.S. at 464-65.

[10] *Id.*

[11] *Id.* at 465.

[12] Katz v. United States, 389 U.S. 347, 351 (1967).

bounds when it listened to the contents of Katz's conversation.[13] The Court developed a new standard—the reasonable expectation of privacy—to determine whether an act by the government constitutes a search, thereby triggering a Fourth Amendment analysis. If a person has "exhibited an actual (subjective) expectation of privacy" and it is one "that society is prepared to recognize as 'reasonable,'"[14] then a search in the constitutional sense has occurred, and the court will subject it to further analysis—usually, determining whether there was a warrant or whether an exception to the warrant requirement applies. If, on the other hand, there was no reasonable expectation of privacy, a warrantless search does not offend the Fourth Amendment.

Although *Katz* established that the contents of a conversation are accorded constitutional protection, the Court did not extend this protection to information generated in making the communication. This issue arose in *Smith v. Maryland*, in which the Court held that a person does not have a reasonable expectation of privacy in the telephone numbers he dials.[15] Michael Lee Smith was a thief who robbed a young woman and then harassed her with obscene phone calls. The police used a pen register (without a warrant) to record the numbers dialed from Smith's office. Based on the numbers he dialed, the police determined that Smith was calling the young woman and later arrested him. In concluding that a search had not occurred, the Court reiterated that a person has no legitimate expectation of privacy in information voluntarily given to third parties—in this case, dialed numbers to the phone carrier.[16]

Generally, the Court has not applied the Fourth Amendment to surveillance conducted in public.[17] Under this theory, the police are permitted to, without a warrant, fly a plane[18] or a helicopter[19] in public airspace over a person's private property to look for illegal activity; photograph commercial property "exposed to visual observation from the air" from a plane that is "lawfully within navigable airspace";[20] and attach a tracking device to a suspect's vehicle to track its movements while in public.[21]

Despite granting police wide latitude for searches occurring in public, the Court remains solicitous of privacy in the home. In *Karo v. United States*, the Court held that monitoring the presence of an item in a private residence through the use of a beeper violated the Fourth Amendment rights of the residents, absent a valid warrant.[22] Likewise, when police, without a warrant, used thermal imaging on Danny Kyllo's home to determine if he was using high-

[13] *Id.* at 352-53.

[14] *Id.* at 361 (Harlan, J., concurring).

[15] Smith v. Maryland, 442 U.S. 735, 745-46 (1979).

[16] *Id.* at 742; *see also* United States v. Miller, 425 U.S. 435, 442-43 (1976) (holding that financial statements and deposit slips transmitted to bank were not protected from police inquiry because they had been turned over to a third party).

[17] Ric Simmons, *Why 2007 Is Not Like 1984: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence*, 97 J. CRIM. L. & CRIMINOLOGY 531, 549 (2007).

[18] California v. Ciraolo, 476 U.S. 207, 215 (1986) (holding that naked-eye search from airplane at 1,000 feet was not a search).

[19] Florida v. Riley, 488 U.S. 445, 451-52 (1989) (holding that surveillance from helicopter at 400 feet was not a search).

[20] Dow Chem. Co. v. United States, 476 U.S. 227, 238-39 (1986).

[21] United States v. Knotts, 460 U.S. 276, 285 (1983). For a more detailed discussion of this case, see *United States v. Knotts*: Surveillance on Public Roadways, *infra* p. 15.

[22] United States v. Karo, 468 U.S. 705, 718 (1984) (upholding introduction of evidence found during search that was based in part on impermissible beeper monitoring; warrant was independently sustainable by additional information).

intensity heat lamps (usually an indication of growing marijuana), the Court again protected the sanctity of the home, holding that information on activities within a home derived through sense-enhancing technology outside of it was obtained in violation of the Fourth Amendment.[23]

The Constitution, however, is just one font of legal standards that balance privacy interests with law enforcement needs. The Constitution is a floor, not a ceiling. Federal law (and state constitutions and statutes) can provide more protection than the Constitution requires, but no less. There are several comprehensive federal statutes that regulate the use of electronic surveillance—in some instances Congress has seen fit to provide more protection than the constitutional floor, while in others it has not.

Federal Surveillance Statutory Framework

As criminal enterprises harness new technologies to commit crime and evade police detection, the police seek to avail themselves of the same technologies in an effort to effectively investigate and prosecute criminal activities. Over the past several years, law enforcement has used cell phone information obtained through service providers to monitor the movements of suspects. Meanwhile, Congress has drawn and redrawn access standards under electronic communication laws. Still, the debate over the use of cell location information is not "*whether* the government can obtain cell site information. Rather, the issue is the *standard* it must meet before a court will authorize such disclosure."[24]

Electronic Communications Privacy Act (ECPA)

In response to *Katz*,[25] Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[26] which is the core of federal domestic surveillance law. Title III prohibits the unauthorized use of surveillance techniques—for instance, bugging and wiretapping—by public and private actors, but permits law enforcement to use such techniques in controlled and well-defined circumstances.[27] In 1986, Congress enacted the Electronic Communications Privacy Act,[28] which amended Title III, to prevent the "unauthorized interception of electronic communications" and "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies."[29] Congress sought to

[23] Kyllo v. United States, 533 U.S. 27, 34 (2001) (holding that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, constitutes a search—at least where (as here) the technology in question is not in general public use") (citation omitted).

[24] *In re* Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Information, No. 06-MISC-004, 2006 U.S. Dist. LEXIS 73324, *2 (E.D. Wis. October 6, 2006).

[25] Matthew Minkle Werdegar, *Lost?* The *Government Knows Where You Are: Cellular Telephone Call Location Technology and the Expectation of Privacy*, 10 STAN. L. & POL'Y REV. 103, 109 (1998).

[26] Omnibus Crime Control and Safe Streets Act of 1968, P.L. 90-351, 82 Stat. 197.

[27] 1 JAMES G. CARR & PATRICIA L. BELLIA, THE LAW OF ELECTRONIC SURVEILLANCE §1.3 (2011).

[28] Electronic Communications Privacy Act of 1986, P.L. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.); *see* CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle; *see also* CARR & BELLIA, *supra* note 27, §1.14.

[29] S.Rept. 99-541, at 1 (1986).

balance the interests of law enforcement with the interest of citizen privacy.[30] There are three main titles in ECPA: the Wiretap Act,[31] the Stored Communications Act,[32] and the Pen Register/Trap Trace Statute.[33]

The first title of ECPA amended Title III of the 1968 Omnibus Crime Control Act, the Wiretap Act, to cover not only wire and oral communications, as originally enacted, but also "electronic communications."[34] Under §2518, the government may obtain a wiretap order and listen to the content of the calls (the words spoken) to and from a suspect only by demonstrating (1) probable cause to believe that a crime was or is being committed; (2) the communication is relevant to that crime; (3) normal investigative procedures have been tried but have failed; and (4) police believe the location from which the communication is made is connected to the crime.[35]

The Pen Register/Trap Trace Statute is found in the second title of ECPA. A "pen register"[36] records numbers dialed from a phone, and a "trap and trace device" captures the telephone number of an incoming call.[37] The pen register and trap-trace devices are the preferred investigatory tools of law enforcement due to the modest standard for justifying their use: the government need only show that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[38] This standard, which is significantly less than probable cause or reasonable suspicion, stems from the theory that a person has no reasonable expectation of privacy in the phone numbers he dials.[39] Under this statute, the court wields no power of review but merely requires that the certificate be in proper form.[40] Though this standard is less demanding, there are limitations to the information that police may seek with a pen register or trap-trace device: neither instrument may be used "in a manner so as to constitute a 'tracking device'" without first showing probable cause.[41]

[30] *Id.* at 5; H.Rept. 99-647, at 19 (1986).

[31] 18 U.S.C. §§2510-2520 (2006).

[32] 18 U.S.C. §§2701-2712 (2006).

[33] 18 U.S.C. §§3121-3127 (2006).

[34] 18 U.S.C. §§2510-2520.

[35] 18 U.S.C. §2518.

[36] 18 U.S.C. §3127(3) (A "pen register" is defined as "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.").

[37] 18 U.S.C. §3127(4) (A "trap and trace device" is defined as "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, provided, however, that such information shall not include the contents of any communication.").

[38] 18 U.S.C. §3123(a)(1).

[39] Smith v. Maryland, 442 U.S. 735 (1979).

[40] *See In re* Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; (2) Authorizing the Release of Subscriber and Other Information; and (3) Authorizing the Disclosure of Location-Based Services, Nos. 1:06-MC-6, 1:06-MC-7, 2006 WL 1876847, *2 (N.D. Ind. July 5, 2006).

[41] *In re* Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d) to Disclose Subscriber Information and Historical Cell Site Information for Mobile Identification Numbers: (XXX) XXX-AAAA, (XXX) XXX-BBBB, and (XXX) XXX-CCCC, 509 F. Supp. 2d 64, 68 (D. Mass. 2007) (citing 47 U.S.C. §1002(a)(2)(B) (2006)).

The third title of ECPA is the Stored Wire and Electronic Communications and Transactional Records Access Act, more commonly referred to as the Stored Communications Act (SCA). Section 2703 of the SCA prescribes the manner in which service providers may divulge records and contents of wire and electronic communications to the government.[42] Under subsections (a) and (b), if the government seeks the *contents* of a communication that has been in storage less than 180 days, it must obtain a warrant (supported by probable cause) under Rule 41 of the Federal Rules of Criminal Procedure.[43] Under §2703(c), if the government seeks only "a record or other information pertaining to a subscriber,"[44] it can require the service provider to turn over the documents if they "offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[45]

The most significant provision of the SCA for purposes of cell location data is the definition of "electronic communication." This definition excludes "any communication from a tracking device,"[46] which is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[47] In the courts that have confronted this issue, much hinges on whether a cell phone should be categorized as a "tracking device."[48]

In 1994, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA), which required communication providers to develop protocols for ensuring law enforcement access to information for which it had lawful authorization.[49] Congress authorized funding for these service providers to assist in upgrading their systems.[50] CALEA required telecommunication carriers to ensure they had the ability to provide law enforcement "access to call-identifying information."[51] It should be noted, however, that the text explicitly excluded location information: "such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)...."[52]

---

[42] 18 U.S.C. §§2703, 2702 (2006) ("A person or entity providing electronic communication service to the public shall not knowingly divulge to any person or entity the contents of the communication while in electronic storage by that service."); *see* CARR & BELLIA, *supra* note 27, §1.17.

[43] 18 U.S.C. §2703(a); FED. R. CRIM. P. 41(d).

[44] 18 U.S.C. §2703(c).

[45] 18 U.S.C. §2703(d).

[46] 18 U.S.C. §2711 (2006) (cross-referencing 18 U.S.C. §2510 for definitions); 18 U.S.C. §2510(12)(C).

[47] 18 U.S.C. §3117 (2006).

[48] Title I of ECPA references the use of tracking devices. 18 U.S.C. §3117(b); *see also* FED. R. CRIM. P. 41 ("After receiving an affidavit or other information, a magistrate judge—or if authorized by Rule 41(b), a judge of a state court of record—must issue the warrant if there is probable cause to search for and seize a person or property or to *install and use a tracking device*.") (emphasis added). Congress included §3117 to ensure that mobile tracking devices could be used when a suspect crosses state lines. The Senate report states that this was merely a jurisdictional clarification that was not intended to affect the legal standards required for tracking authorization. S.Rept. 99-541, at 10 (1986). Section 3117 broadly defines "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. §3117(b). This definition is integral to understanding whether a warrant is needed to obtain locational information from a cell phone; some courts treat cell phones as tracking devices, while others do not.

[49] Communications Assistance for Law Enforcement Act, P.L. 103-414, 108 Stat. 4279 (1994).

[50] H.Rept. 103-827, at 10 (1994).

[51] 47 U.S.C. §1002(a)(2) (2006).

[52] 47 U.S.C. §1002(a)(2)(B).

Evidentiary Standards of Proof Under ECPA

It is helpful to think of the requisite evidentiary proof required for disclosure of electronic communications as a tiered system, ranging from highest (or most stringent) to lowest (or least stringent).[53] The most stringent is the Wiretap Act standard—the "super-warrant" requirement.[54] Among other conditions, the Wiretap Act requires a detailed affidavit of the facts warranting the search, the specific time and date of the proposed search, and an explanation of why other investigatory methods are insufficient.[55] Next are tracking devices, as defined in 18 U.S.C. §3117, which may require a warrant (based upon probable cause) under Rule 41 of the Rules of Criminal Procedure.[56] Below that falls §2703(d) of the Stored Communications Act, which requires "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[57] As discussed below, the courts are split on whether §2703(d) applies to historical records, real-time records, or both. Finally, the lowest tier, contained in the Pen Register/Trap Trace statute, is a certification that the "information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."[58] Police need not present specific facts as the higher tiers require, but

[53] This framework is described in *In re Application for Pen Register and Trap/Trace Device With Cell Site Location Authority*, 396 F. Supp. 2d 747, 753 (S.D. Tex. 2005).

[54] Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 630 (2003).

[55] 18 U.S.C. §2518 (2006).

[56] 18 U.S.C. §3117 (2006). Probable cause, as required for a wiretap or information from a tracking device, is the highest level of evidentiary proof to conduct a search. It is rooted in the text of the Constitution, U.S. CONST. amend IV, and the Court has reiterated time and again that law enforcement must obtain a warrant based upon probable cause unless the investigation does not implicate a reasonable expectation of privacy or else falls within an established exception. Katz v. United States, 389 U.S. 347, 357 (1967) (citations omitted). There are various formulations of this standard, but it is said that "[p]robable cause exists where the facts and circumstances within their [the officers'] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed." Brinegar v. United States, 338 U.S. 160, 175-76 (1949) (citation omitted) (internal quotation marks omitted). The Court later simplified this phrase by requiring a "fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983).

[57] 18 U.S.C. §2703(d) (2006). "Specific and articulable facts" is comparable to the "reasonable suspicion" standard, which was first announced in *Terry v. Ohio*, 392 U.S. 1, 30-31 (1968). Reasonable suspicion requires that the officer "be able to articulate something more than an inchoate and unparticularized suspicion or hunch," United States v. Sokolow, 490 U.S. 1, 7 (1989) (internal quotation marks omitted), but instead has information that a "reasonably prudent man in the circumstances would be warranted in the belief that his safety or that of others was in danger." *Terry*, 392 U.S. at 27.

[58] 18 U.S.C. §3122(b)(2) (2006). The standard for pen registers and trap and trace devices bears some resemblance to the "special needs" doctrine, which covers cases "beyond the normal need of law enforcement." Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 665 (1989) (balancing the "individual's privacy expectations against the Government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context"). This reasonableness standard has been used in cases of drug tests for high school students, Bd. of Educ. of Indep. Sch. Dist. No. 92 v. Earls, 536 U.S. 822, 838 (2002), and railroad employees, Skinner v. Ry. Labor Execs.' Ass'n., 489 U.S. 602, 633-34 (1989), and drunk driving checkpoints, Michigan Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990). But the Court has cabined off the use of this lowest standard to those few limited instances; the Court declined to apply it to a drug interdiction checkpoint, City of Indianapolis v. Edmond, 531 U.S. 32, 48 (2000), and drug tests for birthing mothers, Ferguson v. City of Charleston, 532 U.S. 67, 86-87 (2001). This balancing test is much easier to satisfy than probable cause or reasonable suspicion.

merely must present the certification. This requirement has been described by one federal court as a "low one."[59]

The differences in these standards are important, as the debate in state and federal courts over cell location information turns on which tier—or level of proof—the government must prove to obtain the information; some courts require a showing of probable cause, while others permit an order based on "specific and articulable facts."

Cell Phone Surveillance in the Courts

Federal electronic surveillance law is a patchwork of terms and standards. Nowhere is this more apparent than in the federal courts' application of ECPA to government requests for cell site location information.[60] Policy arguments exist both for facilitating access and restricting it. The government, on one hand, argues that "cell site information is an important investigatory tool which is used ... to, among other things, help to determine where to establish physical surveillence [sic] and to help locate kidnapping victims, fugitives, and targets of criminal investigations."[61] Privacy proponents, on the other hand, want to ensure "Big Brother stays out of your pocket" and argue that the government is trying to turn the cell phone system into a "vast network for warrantless physical surveillance."[62]

---

[59] *In re* Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace, 405 F. Supp. 2d 435, 439 (S.D.N.Y. 2005).

[60] *See* Congressional Distribution Memorandum, *Legal Standard for Disclosure of Cell-Site Information (CSI) and Geolocation Information*, by Gina Stevens, Alison Smith, and Jordan Segall (on file with CRS). The debate in the federal courts centers around cell site location information, which is one of the two distinct methods for determining the location of a cell phone. (A full description of cell phone technology is beyond the scope of this report, but can be found at Marshall Brain et al., *How Cell Phones Work*, HOW STUFF WORKS (last visited October 20, 2011), http://electronics.howstuffworks.com/cell-phone.htm). GPS, or Global Positioning System, is a system of 24 satellites that constantly orbit Earth. *In re* Application of the United States of America for Historical Cell Site Data, 747 F. Supp. 2d 827, 831 (S.D. Tex. 2010). When hardware inside the cell phone receives signals from at least four of these satellites, the handset can calculate its latitude and longitude to within 10 meters. *Id.* at 832. There are drawbacks to GPS technology: the system is not fully operable when objects block its access. Note, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J. L. & TECH. 307, 308 (2004). Despite the accuracy of this technology, courts have yet to address whether GPS tracking can be used to locate a cell phone's location. Adam B. Merrill, Comment, *Can You Find Me Now? The Federal Government's Attempt to Track Criminal Suspects Using Their Cell Phones*, 43 ARIZ. ST. L. J. 591, 606 (2011).

The second method of determining the location of a cell phone is by triangulation, a process by which a cell phone's location can be determined from its communication with local cell towers. *See In re* Pen Register & Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 751 (S.D. Tex. 2005). There are two distinct technologies used to locate a cell phone through a network: time difference of arrival and the angle of arrival. Note, *Who Knows Where You've Been?*, 18 HARV. J. L. & TECH. 307, 308 (2004). The time difference technology measures the time it takes for a signal to travel from the cell phone to the tower. When multiple towers pick up this signal, an algorithm allows the network to determine the phone's latitude and longitude. *Id.* at 308-09. The angle of arrival technology uses the angles at which a phone's signal reaches a station. When more than one tower receives the signal, the network compares this data the multiple angles of arrival and triangulates the location of the cell phone. *Id.* at 309.

[61] *In Re* Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F. Supp. 2d 448, 452 (S.D.N.Y. 2006) (quoting Gov. Br. at 2).

[62] *Cell Tracking*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/cell-tracking (last visited October 19, 2011); *see also* Brian C. Davis, Note, *An Un-Watchful Eye: How Courts Have Allowed Emerging Electronic Surveillance Escape Fourth Amendment Protection*, 46 NEW ENG. L. REV. (Forthcoming 2012) (on file with the New England Law Review) ("[I]f the government decides to use these devices, they must comply with the safeguards entrenched in the Fourth Amendment.").

Though these requests for cell site location information have become more frequent in the lower courts, only one circuit has directly confronted the issue of cell location information. The Third Circuit Court of Appeals decided in favor of the government, holding that the "specific and articulable facts" standard of the Stored Communications Act (SCA) was sufficient to obtain cell location information. Many magistrate judges, on the other hand, have rejected this approach, instead requiring probable cause. At times, the outcome in the lower courts has been influenced by whether the government was seeking historical versus prospective cell site information.[63]

Third Circuit Approach

In 2010, the Third Circuit confronted as a matter of first impression a government request for historical cell location information.[64] The government applied for a court order under the Stored Communications Act to compel a cell phone service provider to produce a customer's historical cellular tower data relating to that customer's location.[65] In a lengthy opinion, the magistrate judge had denied this request, concluding that an order of this type, whether historical or real-time, could only be granted upon a showing of probable cause.[66] The District Court, without analysis, affirmed the magistrate judge's opinion.[67] The Third Circuit reversed, holding that the magistrate judges have the discretion whether to require the government to show "specific and articulable facts" under the Stored Communication Act or probable cause under a general warrant theory, depending on whether access to this information under the lower "articulable facts" standard would violate the Fourth Amendment.[68]

Before the lower court, the government primarily contended that a cell phone was not a tracking device and thus cell location information could be obtained under the Stored Communications Act.[69] This proposition was crucial to the government's argument because location information from a "tracking device"[70] cannot be sought under the Stored Communications Act.[71] If this

[63] Some cases hold that historical but not prospective information can be obtained under the Stored Communications Act. *See In re* Application for Pen Register and Trap/Trace Device with Cell Location Authority, 396 F. Supp. 2d 747 (S.D. Tex. 2005); *In re* United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 396 F. Supp. 2d 294 (E.D.N.Y. 2005). Others hold that historical information and limited prospective information can be obtained under the SCA. *See In re* Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Information, 622 F. Supp. 2d 411 (S.D. Tex. 2007). Finally, others permit access to both prospective and historical information. *See In re* Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F. Supp. 2d 448 (S.D.N.Y. 2006).

[64] The information sought in this case was not from a GPS device; the court was not asked nor did it take a position on the use of GPS data, but merely answered the cell location information question. *In re* Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304, 311 (3d Cir. 2010).

[65] *Id.* at 305.

[66] *In re* Application of the United States of America for an Order Directing Provider of Electronic Communication Service to Disclosure Records to the Government, 534 F. Supp. 2d 585, 585-86 (W.D. Pa. 2008).

[67] *In re* Application of the United States of America for an Order Directing Provider of Electronic Communication Service to Disclose Records to the Government, No. 07-524M, 2008 U.S. Dist. LEXIS 98761 (W.D. Pa. September 10, 2008).

[68] *Application for Disclosure of Records*, 620 F.3d at 319.

[69] *Application for Disclosure of Records,* 534 F. Supp. 2d at 601.

[70] 18 U.S.C. §3117(b).

[71] To be clear, the definition of "electronic communications" excludes "any communication from a tracking device," 18 (continued...)

argument failed, the government would be required to show probable cause. A tracking device, the magistrate judge noted, is anything which "permits the tracking of movement of a person or object."[72] She concluded that a cell phone undoubtedly constituted a "tracking device" because it could locate a person to within 50 feet and continuously broadcasted information.[73] She further pointed out that "[b]y virtue of cell phone technology, law enforcement may now electronically monitor our movements with as much—indeed, ofttimes more—scope and precision as by its traditional methods of visual surveillance and/or installation of a 'beeper.'"[74]

Because the cell phone was considered a tracking device, and the Stored Communications Act excludes tracking devices from its reach, the magistrate judge concluded that the Stored Communications Act could not govern this request, and therefore any retrieval of information must be authorized under the normal warrant process as required by Rule 41 of the Federal Rules of Criminal Procedure.[75]

On appeal from the district court, the government narrowed its focus, arguing that historical cell location information (rather than both historical and prospective information) falls within the Stored Communications Act. The Third Circuit agreed, reversed the lower courts, and held that the Stored Communications Act's intermediate "articulable and specific facts" standard applied.[76] The government's main contention was again that cell phones were not tracking devices, but, further, that the location data was derived not from an "electronic communication,"[77] but from a "wire communication."[78] "'Wire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception...."[79] The Third Circuit accepted that the historical location information requested was "derived from a 'wire communication' and does not itself comprise a separate 'electronic communication.'"[80] Even if a cell phone was a tracking device excluded from "electronic communication" as described in §2510, it would not matter, as tracking devices are not excluded from the definition of "wire communication."[81] Relying on the phrase "may be issued" in §2703(d), the court concluded that the decision whether to require a warrant or an order under the intermediate standard is

(...continued)

U.S.C. §2510(12)(C). The definition of "wire communications," the other form of communications governed by the Stored Communications Act, does *not* exclude communications from a tracking device. 18 U.S.C. §2510(1).

[72] *Application for Disclosure of Records*, 534 F. Supp. 2d at 601 (quoting 18 U.S.C. §3117(b)).

[73] *Id.* at 602.

[74] *Id.*

[75] *Id.* at 601.

[76] *Application for Disclosure of Records*, 620 F.3d at 319.

[77] ECPA defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. §2510(12).

[78] *Id.* at 309.

[79] 18 U.S.C. §2510(1). "'Aural transfer' means a transfer containing the human voice at any point...." §2510(18). Meanwhile, "electronic communication" does not include "any wire or oral communication...." §2510(12). "Oral communication" means an utterance by a person with a justifiable expectation that the communication will not be intercepted. §2510(2).

[80] *Application for Disclosure of Records*, 620 F.3d at 310.

[81] *Id.*

discretionary—that is, a court can choose to require either a warrant or a court order based on the lesser standard, depending on the facts.[82]

Conflict in the Lower Courts

Though the other circuit courts have yet to interpret the requests for cell phone location information under the Stored Communications Act, the district courts, and in particular magistrate judges, have written quite lengthy opinions on the issue, and have reached divergent conclusions.

For instance, the Southern District of Texas found unpersuasive the government's stance that the Stored Communications Act applied to its request for prospective or real-time cell location information.[83] The analysis, similar to that employed by the magistrate judge in the Third Circuit case, begins with the definition of tracking device: the government argued that cell location information did not fit the definition of tracking device—"an electronic or mechanical device which permits the tracking of the movement of a person or [object]"[84]—since it did not provide detailed location information. With the advance in cell phone technology, the court found this argument wanting, as tracking was becoming very precise, and further because the definition of tracking device does not differentiate between general and specific vicinity tracking.[85] Holding that a cell phone falls into the definition of "tracking device," the court then analyzed each major section of ECPA—the Pen Register/Trap Trace Statute, the Wiretap Act, and the Stored Communications Act—to determine if any of the sections apply to cell location information.

The court dismissed this information as obtainable under the Pen Register Statute, noting that Congress explicitly prohibited law enforcement from obtaining any location information under this statute.[86] Next, the court excluded the "super-warrant wiretap standard," as the government was not seeking to obtain the *contents* of the defendant's conversations, but rather the *location* of the caller.[87] Finally, the court eliminated the Stored Communications Act based on the definitions used in that act. First, the SCA must apply to an "electronic communication service." "Electronic communication service," in turn, is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[88] This location information cannot

[82] *Id.* at 315. This interpretation of §2703(d) has not gone unscathed. Professor Orin Kerr regards this theory as "quite unpersuasive." Orin Kerr, *Third Circuit Rules that Magistrate Judges Have Discretion to Reject non-Warrant Court Order Applications and Require Search Warrants to Obtain Historical Cell-Site Records*, THE VOLOKH CONSPIRACY, http://volokh.com/2010/09/08/third-circuit-rules-that-magistrate-judges-have-discretion-to-reject-court-order-application-and-require-search-warrants-to-obtain-historical-cell-site-records/ (last visited October 4, 2011). Kerr cites to *Ex parte United States*, 287 U.S. 241 (1932), noting that "magistrate judges do not have discretion to decide whether to issue court orders if the government satisfies the legal threshold." *Id.* If the court were given discretion whether to require a warrant, law enforcement could then forum shop for the more lenient magistrate. *Id.*

[83] *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 759, n.16 (S.D. Tex. 2005) (noting that historical cell location, as compared to prospective information, fits the definition of transactional records covered by the Stored Communications Act).

[84] *Id.* (citing 18 U.S.C. §3117(b) (2006)).

[85] *Id.* at 755.

[86] *Id.* at 757-58 ("With regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices ... such call identifying information **shall not include any information that may disclose the physical location of the subscriber** (except to the extent that the location may be determined from the telephone number).") (emphasis in original) (quoting 47 U.S.C. §1002(a)(2)).

[87] *In re Application*, 396 F. Supp. 2d at 758.

[88] 18 U.S.C. §2510(15).

be from an electronic communication, the court concluded, as the definition specifically excludes "tracking devices." It also cannot be a "wire communication" because a wire communication involves the "human voice."[89] Based on this logical sequence of interlocking definitions, the court held that the SCA did not apply, and that the traditional warrant would be necessary.[90]

This analysis by the Southern District of Texas has been followed in a majority of jurisdictions.[91] A minority of courts, on the other hand, have held that the government need not establish probable cause, relying primarily on the hybrid theory.

Hybrid Theory

Under the hybrid theory, the government purports to have authority to obtain prospective cell location information by combining provisions of the Pen Register Statute and the Stored Communications Act.[92] The Pen Register Statute was traditionally used by law enforcement to record the dialed numbers for outgoing calls, and the trap and trace device to record incoming calls.[93] Pen registers are used not only for recording telephone numbers dialed but also to record "signaling information,"[94] language that was expanded by the USA PATRIOT Act in 2001.[95] To get approval under the Pen Register Statute, law enforcement need only show that the material requested is relevant to an ongoing investigation.[96] Although cell location information may fit within this definition of "signaling information," the Communications Assistance for Law Enforcement Act (CALEA) of 1994 prohibits government access to location disclosing information gained "solely pursuant to the authority for pen registers and trap and trace devices ..."[97] Some courts rely on this "solely pursuant" language, or "exception clause," to conclude that

[89] *Id.* at 759.

[90] *Id.* at 759, 765.

[91] *See In re* Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 2006 U.S. Dist. LEXIS 11747, *2 (S.D.N.Y. 2006); *In re* Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Information, 412 F. Supp 2d 947 (E.D. Wis. 2006); *In re* Application for Pen Register and Trap/Trace Device With Cell Site Location Authority, 396 F. Supp. 2d 294 (E.D.N.Y. 2005); *In re* Application of the United States of America for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 384 F. Supp. 2d 562 (E.D.N.Y. 2005).

[92] *See* Lisa M. Lindemenn, Note, *From Cell to Slammer: Flaws in the Hybrid Theory*, 53 ARIZ. L. REV. 663, 672 (2011).

[93] 18 U.S.C. §3127(3)-(4) (2006).

[94] *In re* Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace, 405 F. Supp. 2d 435, 438 (S.D.N.Y. 2005); 18 U.S.C. §3127(3)-(4).

[95] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, P.L. 107-56, §216(c)(2), 115 Stat. 272, 290.

[96] 18 U.S.C. §3123(a)(1) (2006).

[97] 47 U.S.C. §1002. This section reads, in pertinent part:

> a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of—...
>
> (2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-indentifying information that is reasonably available to the carrier—
>
> (A) before, during, or immediately after the transmission of a wire or electronic communication (or such later time as may be acceptable to the government); and

(continued...)

the Pen Register/Trap Trace Statute may not be used as the sole means for obtaining cell location information but can be used in conjunction with another statutory mechanism.

The hybrid theory looks to the Stored Communications Act as that other mechanism. Section 2703(c)(1) of the SCA provides that "a governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service."[98] Cell location information, the theory goes, is information that pertains to a subscriber of cellular phone service.[99] There is, however, a roadblock to this theory: cell location information may appear to derive from an "electronic communication" from a cell phone to a cell tower, but the act excludes any communication from a tracking device from an "electronic communication."

As was shown above, the definition of electronic communication excludes any "communication from a tracking device."[100] Thus it may seem that cell phone tracking information cannot be obtained under this theory. Courts accepting the hybrid theory, however, have pointed out that "information on the location of cell towers is not the 'service' to which a cellular customer subscribes. Instead, the user subscribes to the voice—and perhaps data—transmission capabilities provided by the cellular carrier."[101] By focusing on the type of service the customer subscribes to, and not the nature of the location information being relayed, the hybrid theory overcomes this attack.

There is another hurdle to the hybrid theory: it is argued that the Stored Communications Act was intended to cover only historical, not prospective information.[102] To surmount this limitation, the theory "circles back to the Pen/Trap statute ... [and] asserts that disclosure of cell site location information is authorized by the SCA and can be collected in real time by virtue of the Pen/Trap Statute."[103] With those concerns arguably overcome, the courts rely on §2703(d)'s "specific and articulable facts" standard as controlling these requests.

The Eastern District of New York is not alone in accepting this theory,[104] but most jurisdictions have rejected it.[105] Relying on legislative history, at least one court has noted that CALEA was never intended to expand the reach of existing surveillance law.[106]

(...continued)

> (B) in a manner that allows it to be associated to which it pertains,
>
> except that, with regard to information acquired *solely pursuant* to the authority for pen registers and trap and trace devices (as defined in section 3127 of Title 18), and such call identifying information *shall not include any information that may disclose the physical location of the subscriber* (except to the extent that the location may be determined from the telephone number); (emphasis added).

[98] 18 U.S.C. §2703(c)(1) (2006).

[99] *In re Application for Disclosure of Telecommunications Records*, 405 F. Supp. 2d at 444-45.

[100] 18 U.S.C. §2510(12) (2006).

[101] *In re Application for Disclosure of Telecommunications Records*, 405 F. Supp. 2d at 446.

[102] *In re* Application for Pen Register and Trap/Trace Device With Cell Site Location Authority, 396 F. Supp. 2d 747, 753 (S.D. Tex. 2005).

[103] *See* Lindemenn, *supra* note 92, at 675.

[104] *See In re* Application of the United States for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Information and/or Cell-Site Information, 411 F. Supp. 2d 678, 680 (W.D. La. 2006); *In re* Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F. Supp. 2d 448 (S.D.N.Y. 2006).

A majority of the courts require law enforcement to obtain a warrant to access cell location information. But it should be noted that there has been little appellate case law on cell phone tracking, as there appears to be no incentive for defendants to raise the issue—ECPA does not contain an exclusionary rule to prevent the admission of improperly obtained evidence.[107] Thus far, only the Third Circuit has directly ruled on this issue.

Governmental Surveillance of Vehicles

Like surveillance of cell phone location, the government uses GPS devices to track the location of vehicles.[108] Again, the courts have been asked to reconcile privacy interests and the needs of law enforcement in an age of emerging technology. In contrast to the cell phone tracking cases, the vehicle tracking cases have focused on constitutional and not statutory provisions.

(...continued)

[105] *In re* Applications of the United States for Orders Authorizing the Disclosure of Cell Site Information, Nos. 05-403, 05-404, 05-407, 05-408, 05-409, 05-410, 05-411, 2005 WL 3658531, at *1 (D.D.C. October 26, 2005); *In re* Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register a Caller Identification System on Telephone Numbers [Sealed] and [Sealed] and the Production of Real Time Cell Site Information, 402 F. Supp. 2d 597 (D. MD. 2005); *In re* Application of the United States for and Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, No. 06 CRIM. MISC. 01, 2006 WL 468300, at *2 (S.D.N.Y. February 28, 2006); *In re* Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Information, 412 F. Supp. 2d 947, 949 (E.D. Wis. 2006).

[106] The Director of the Federal Bureau of Investigation (FBI) testified before Congress during its consideration of CALEA, and insisted that the Pen Register/Trap Trace Statute has "'nothing to do with' the Stored Communications Act, and that transactional information is 'exclusively dealt with in chapter 121 of Title 18.'" *In re Application*, 396 F. Supp. 2d 747, 753 (S.D. Tex. 2005) ("The government's hybrid theory, while undeniably creative, amounts to little more than a retrospective assemblage of disparate statutory parts to achieve a desired result."); *see Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings Before the Subcomm. on Technology and Law of the Senate Committee on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Committee on the Judiciary*, 103rd Cong. 32 (statement of Director Freeh):

> First, as is clearly set forth in the "purpose" section of the proposed legislation, the intent of the legislation is to maintain existing technical capabilities and to "clarify and define the responsibilities of common carriers *** to provide the assistance required to ensure that government agencies can implement court orders and lawful authorizations to intercept the content of wire and electronic communications and acquire call setup information *under chapters 119 and 206 of Title 18 and chapter 36 of Title 50.*" (emphasis added.) These chapters have nothing to do with "transactional information" under our federal electronic surveillance and privacy laws. All telecommunications "transactional" information is already protected by federal law and is exclusively dealt with in chapter 121 of Title 18 of the United States Code ("stored wire and electronic communications and transactional records access"). The proposed legislation does not relate to chapter 121 of Title 18. Second, under federal law, Congress treats law enforcement's use of pen registers and dialing information differently than "transactional information"—such as detailed telephone *billing* information.

[107] Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 681 (2011).

[108] CRS Report R41663, *Law Enforcement Use of Global Positioning (GPS) Devices to Monitor Motor Vehicles: Fourth Amendment Considerations*, by Alison M. Smith.

United States v. Knotts: Surveillance on Public Roadways

In *United States v. Knotts*, law enforcement attached a tracking device to a can of chloroform, which was subsequently transported by the defendant in his car to a secluded cabin.[109] The police used the tracking device to learn of his location and then obtained a warrant based on this information.[110] When executing the search at the cabin, the police found a drug laboratory and materials to make illegal drugs.[111] The question presented was whether this monitoring violated the defendant's Fourth Amendment rights. The Supreme Court held that since a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," this type of monitoring did not violate the defendant's Fourth Amendment rights.[112] The Court further stated that "scientific enhancement of this sort raises no constitutional issues which visual surveillance would not raise."[113] According to *Knotts*, if the police could theoretically track a suspect by the naked eye, they can use technology to do the same thing.

United States v. Karo: Surveillance on Private Property

In *United States v. Karo*, the Court confronted the issue of "whether the monitoring of beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence."[114] In *Karo*, Drug Enforcement Administration (DEA) agents attached a tracking device to a can of ether and tracked the can's movements between multiple private residences and storage facilities.[115] The agents obtained a warrant to search a house rented by one of the defendants based on the information derived from the tracking device.[116] In concluding that use of the tracking device constituted an unreasonable search, the Court first spelled out basic Fourth Amendment principles: "private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable."[117]

Unlike *Knotts*, the Court refused to accept the idea that the government "should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, whether a particular article—or a particular person, for that matter—is in an individual's home at a particular time."[118] This case was distinguishable from *Knotts* because the "information obtained

[109] United States v. Knotts, 460 U.S. 276, 278-79 (1983).

[110] *Id.* at 279.

[111] *Id.*

[112] *Id.* at 281.

[113] *Id.* at 285.

[114] United States v. Karo, 468 U.S. 705, 714 (1984). Though the monitoring of the can of ether while in the private residence was deemed unconstitutional, the warrant permitting police to search the residence where the contraband was found was upheld because the police had sufficient untainted evidence independent of this monitoring. *Id.* at 721.

[115] *Id.* at 708.

[116] *Id.* at 710.

[117] *Id.* at 714.

[118] *Id.* at 716.

in *Knotts* was 'voluntarily conveyed to anyone who wanted to look.'"[119] This gets back to the idea that information a person voluntarily gives to another person—whether it is one's public location or telephone numbers dialed (think *Smith v. Maryland*)—is no longer private and no longer afforded Fourth Amendment protection.

These two decisions left unresolved several lingering issues. Is the public versus private distinction a bright-line rule? Is prolonged surveillance permissible so long as it could have been done by visual surveillance? Does the use of advanced technology, such as GPS that enhances a police officer's senses, ever affect a Fourth Amendment analysis? The courts of appeals were quickly asked to answer these questions.

GPS Tracking in the Seventh and Ninth Circuits

The Seventh and Ninth Circuits have held that the use of a GPS tracking device is not a search afforded Fourth Amendment protection. In *United States v. Garcia*, Judge Posner analogized GPS surveillance to "cameras mounted on lampposts or satellite imaging,"[120] which are not considered searches. The Seventh Circuit, however, was not confronted with the question as to whether *all* tracking of vehicles on public ways is permissible, as the defendant did not raise this issue on appeal. The court did say that the activity at issue, "namely following a car on a public street, ... is unequivocally *not* a search within the meaning of the amendment."[121]

In *United States v. Pineda-Moreno*, law enforcement entered Pineda-Moreno's property and attached a GPS device to his vehicle while it was parked in his driveway.[122] Pineda-Moreno challenged this monitoring not on the basis that the surveillance's continuity exceeded *Knotts* in scope, but rather that police were not permitted to use technology not in general public use as described in *Kyllo v. United States*.[123] Again, the Ninth Circuit rejected this argument, stating that just because GPS made the police more effective at tracking the suspect does not mean that this new form of tracking is unconstitutional; it refused to "equate[] efficiency with unconstitutionality...."[124]

United States v. Jones: Supreme Court Review

The Supreme Court confronts the issue of government tracking once again in *United States v. Jones*.[125] Using an expired warrant, an FBI task force attached a GPS tracking device to Jones's Jeep Grand Cherokee while it was parked in a public lot in Maryland.[126] For four weeks, the government tracked the movements of Jones's car with an accuracy to within 50-100 feet.[127]

[119] *Id.* at 715.

[120] United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007).

[121] *Id.*

[122] United States v. Pineda-Moreno, 591 F.3d 1212, 1213 (9th Cir. 2010).

[123] *Id.* at 1216.

[124] *Id.*

[125] United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *cert. granted sub nom.* United States v. Jones, 131 S. Ct. 3064 (2011) (No. 10-1259).

[126] Brief for Respondent at 4, *Jones*, 131 S. Ct. 3064 (2011) (No. 10-1259), 2011 WL 4479076.

[127] Brief for Petitioner at 3-4, *Jones*, 131 S. Ct. 3064 (2011) (No. 10-1259), 2011 WL 3561881.

Based on this surveillance, the government retrieved over 2,000 pages of GPS data and was able to track Jones to a stash house in Maryland where it ultimately found large amounts of cocaine.[128] Prior to his trial, Jones filed a motion to suppress this evidence, which was denied except for evidence obtained while his vehicle was parked in his garage.[129]

Jones appealed the constitutionality of both the installation and the subsequent surveillance of his movements. The D.C. Circuit Court of Appeals did not address the installation issue, but instead reversed on the basis that a prolonged, 24-hour surveillance without a warrant was a search, and thus violated Jones's Fourth Amendment right to privacy.[130] The government argued this case was on all fours with *Knotts*—that a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[131] Jones argued that the use of a GPS is much more pervasive than the beeper used in *Knotts*, and that society is likely to recognize an expectation of privacy in the "pattern, or sum total, of an individual's daily activities."[132] The D.C. Circuit, accepting Jones's argument, relied on Justice Rehnquist's dicta in *Knotts* that further Court oversight could be triggered under different circumstances: "if [a] dragnet-type law enforcement practice[] as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[133] Ultimately, the D.C. Circuit held that "[s]ociety recognizes Jones's expectation of privacy in his movements over the course of a month as reasonable, and the use of the GPS device to monitor those movements defeated that reasonable expectation."[134]

The Supreme Court has granted certiorari in *Jones* based upon two distinct questions: (1)"Whether the warrantless use of a tracking device on respondent's vehicle to monitor its movements on public streets violated the Fourth Amendment"; and (2) "Whether the government violated respondent's Fourth Amendment rights by installing the GPS tracking device on his vehicle without a valid warrant and without his consent."[135]

As to the first question, much of the debate swirls around Justice Rehnquist's dragnet passage in *Knotts*, and whether he was referring to a program of mass surveillance of the public or prolonged surveillance of a single person.[136] In its brief, the government notes that the Court has used the term "dragnet" to refer to "mass or widespread searches or seizures that are conducted without individualized suspicion," and should not be applied to surveillance of a single individual.[137] Jones counters by noting that "'dragnet' can refer to 'any system for catching a person, esp. a

[128] Brief for Respondent, *supra* note 126, at 5.

[129] United States v. Jones, 451 F. Supp. 2d 71, 88 (D.D.C. 2006).

[130] United States v. Maynard, 615 F.3d 544, 555-56 (D.C. Cir. 2010).

[131] *Id.* at 556.

[132] Brief for Appellants at 65 n.239, *Maynard*, 615 F.3d 544 (D.C. Cir. 2010) (Nos. 08-3030, 08-3034), 2009 WL 3155141 (quoting Recent Case, *Constitutional Law—Fourth Amendment—Seventh Circuit Holds that GPS Tracking is Not a Search.—United States v. Garcia, 474 F.3d 994 (7th Cir. 2007), Reh'g and Suggestion for Reh'g Denied, No. 06-2741, 2007 U.S. App. LEXIS 8397 (7th Cir. Mar. 29, 2007)*, 120 Harv. L. Rev. 2230, 2235 (2007)).

[133] United States v. Knotts, 460 U.S. 276, 284 (1983).

[134] *Maynard*, 615 F.3d at 563.

[135] United States v. Maynard, 615 F.3d 544, 555-56 (D.C. Cir. 2010), *cert. granted sub nom.* United States v. Jones, 131 S. Ct. 3064 (2011) (No. 10-1259) (oral argument held on November 8, 2011).

[136] It should be noted that this passage was dicta, meaning it is not controlling but merely persuasive.

[137] Brief for Petitioner, *supra* note 127, at 34.

fugitive.'"[138] This dragnet theory should not be limited solely to mass surveillance, Jones argues, but should cover prolonged, warrantless surveillance of one person. This question also implicates the public-private dichotomy and whether use of sensory-enhancing technology can turn an otherwise constitutionally permitted investigation into an unconstitutional search. The government argues that the use of technology to collect information in public "does not make the information any less public."[139] Based on that assumption, *Knotts* would apply and the GPS surveillance would not be a search. Jones argues, to the contrary, that the government can obtain information through GPS surveillance to a degree not feasible through visual surveillance. This pattern information is more intrusive than a general search, thus interfering with an individual's reasonable expectation of privacy.

As to the second question, the D.C. Circuit did not reach the issue of whether the installation of the GPS device on Jones's Jeep was in and of itself a Fourth Amendment violation. The Ninth Circuit has held that attachment of a GPS device on a vehicle while parked in the suspect's driveway was not a Fourth Amendment violation, as the car was parked in an area open to public view and the suspect had not exhibited an expectation of privacy in the undercarriage of his car.[140] Using similar reasoning, the Fifth Circuit held that the government's attachment of a GPS device to a car in a public place did not violate the suspect's Fourth Amendment rights, as the car was parked in plain view and the monitoring did not intrude on the suspect's privacy.[141] The First Circuit, on the other hand, held that attaching a tracking device on a vehicle in a public parking lot violates the Fourth Amendment.[142]

Pending Legislation Before the 112th Congress

Several bills have been introduced in the 112th Congress to amend federal surveillance laws.[143] A broad coalition of industry and privacy advocates including Apple, Google, AT&T, the American Civil Liberties Union, and the Constitution Project—dubbed the Digital Due Process Coalition—has joined to advocate for the passage of these measures.[144] The Department of Justice also advocates a clarification of existing surveillance law, but supports a lower standard that would impose a lesser burden on law enforcement.[145]

---

[138] Brief for Respondent, supra note 126, at 44 fn.8 (citing The Living Webster Encyclopedic Dictionary of the English Language 300 (1975)).

[139] Brief for Petitioner, *supra* note 127, at 19.

[140] United States v. McIver, 186 F.3d 1119, 1126-27 (9th Cir. 1999).

[141] United States v. Michael, 645 F.2d 252, 256 (5th Cir. 1981).

[142] United States v. Moore, 562 F.2d 106, 112-113 (1st Cir. 1977).

[143] Senator Al Franken has introduced the Location Privacy and Protection Act of 2011 (S. 1223)—similar to the GPS bill, but which applies only to private, not governmental, actors. Because it only applies to private actors, and this report focuses on governmental tracking, it will not be discussed.

[144] DIGITAL DUE PROCESS, http://www.digitaldueprocess.com (last visited October 19, 2011). The group's official mission statement is "to simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public." *Id.* at http://www.digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163.

[145] The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age, 112th Cong. (2011) (statement of James A. Baker, Assoc. Dep. Att'y Gen., Dep't of Justice) ("Courts' conflicting interpretations of the statutory basis for obtaining prospective cell-site information have created uncertainty regarding (continued...)

Electronic Communications Privacy Act Amendments Act of 2011 (S. 1011)

On May 17, 2011, Senate Judiciary Chairman Patrick Leahy introduced legislation to update federal surveillance law, with a focus on protecting consumer privacy.[146] The Electronic Communications Privacy Act Amendments Act of 2011 (S. 1011) would amend numerous provisions of ECPA, including the Stored Communications Act.[147]

Section 5 would prohibit the government from accessing or using a device to acquire geolocation information, unless the government obtains a warrant based upon probable cause or a court order under Title I or Title IV of the Foreign Intelligence Surveillance Act (FISA) of 1978. There are two exceptions to this requirement for court authorization: (1) to respond to an emergency call by the user of the device; and (2) if the owner of the device gives express consent.

In an emergency, law enforcement may acquire geolocation information if it is determined that an emergency situation exists that (1) involves immediate danger of death or serious bodily injury to another person, conspiratorial activities characteristic of organized crime, or an immediate threat to national security; (2) requires the accessing of geolocation before a court order could be obtained; and (3) there are adequate grounds upon which a court order could be obtained. If law enforcement accesses information based on this emergency exception, it must then apply for a warrant within 48 hours of accessing the information. If a warrant is not obtained, this activity must terminate immediately. If evidence is obtained in violation of this law, an exclusionary clause will apply, which requires that this evidence not be admitted at trial.

Providers of electronic communication services, remote computing service, or geolocation information service would be required to assist law enforcement with accessing the geolocation information permitted under a lawfully obtained warrant. The service providers would in turn be compensated for reasonable expenses incurred in providing such information. Providers are also given immunity from suit for releasing information to the government pursuant to a request under this act.

Section 6 would prohibit the government from requesting contemporaneous or prospective geolocation information from a service provider unless the government met the same warrant standards—that is, obtained a warrant under Rule 41 of the Federal Rules of Criminal Procedure. This act, however, would allow law enforcement to access historical geolocation information based upon a proof of "specific and articulable facts," the same standard contained in the Stored Communications Act.

The bill also permits law enforcement to retrieve general information about the target of the search on a lesser showing, including the name and address of the subscriber, the times and

(...continued)

the proper standard for compelled disclosure of cell-location information, and some courts' requirement of probable cause has hampered the government's ability to obtain important information in investigations of serious crimes. Legislation to clarify and unify the legal standard and the proper mechanism for obtaining prospective cell-site information could eliminate this uncertainty.").

[146] Though this bill targets both governmental and private, third-party use of geolocation information, the private use is beyond the scope of this report.

[147] S. 1011, 112th Cong., 1st Sess. (2011).

durations of calls, and the means and source of payment, but expressly excluding location information. Currently, the law permits access to a "record or other information pertaining to a subscriber...."[148] S. 1011 specifies which records could be accessed by law enforcement.

Geolocational Privacy and Surveillance Act (GPS Bill; S. 1212 and H.R. 2168)

On June 15, 2011, Senator Ron Wyden and Representative Jason Chaffetz introduced companion bills, the Geolocational Privacy and Surveillance Act, or GPS bill.[149] The GPS bill would clarify and establish the standards the government must meet to monitor an individual's movements.

Under the GPS bill, law enforcement's sole means for acquiring geolocation information would be pursuant to a warrant under Rule 41 of the Federal Rules of Criminal Procedure or the Foreign Intelligence Surveillance Act (FISA) of 1978.[150] It would appear that the Stored Communications Act or the Pen Register/Trap and Trace Act would no longer be mechanisms for acquiring this information.

The bill contains a broad prohibition against the disclosure or use of geolocation information.[151] Specifically, it makes it unlawful for any person[152] to (A) intentionally intercept geolocation information pertaining to another person; (B) intentionally disclose geolocation information pertaining to another person when it is known that information was obtained in violation of the act; (C) intentionally use any geolocation information knowing that the information was obtained in violation of the act; or (D) intentionally disclose information that was lawfully obtained under the act, but not authorized to be released to third parties.[153]

There are several exceptions to the prohibition against the use of geolocation information. Providers of geolocation information service[154] may intercept, use, or disclose geolocation information in the normal course of business when it is a "necessary incident to the rendition of service or to the protection of the rights or property of the provider of that service." The service providers, however, shall not randomly monitor customers except to service their systems.

---

[148] 18 U.S.C. §2703(c).

[149] S. 1212, H.R. 2168, 112th Cong., 1st Sess. (2011).

[150] S. 1212, §5.

[151] "Geolocation information" is defined as "any information, that is not the content of a communication, concerning the location of a wireless communication device or tracking device (as that term is defined section 3117) that, in whole or in part, is generated by or derived from the operation of that device and that could be used to determine or infer information regarding the location of the person." S. 1212, §2601(4). "Geolocation information" covers information from both GPS tracking and tracking via cell site location information.

[152] The bill prohibits use of this information by "any person" (*e.g.,* individuals, telecommunications companies, Internet service providers, website operators, etc.), and not solely government actors. However, private use of geolocation information is beyond the scope of this report; this analysis of S. 1212 is limited to government access to geolocation information.

[153] S. 1212, §2602(a)(1). Currently there is no broad federal prohibition against the use of geolocation information.

[154] "Geolocation information service" is defined as "the provision of a global positioning service or other mapping, locational, or directional information service to the public, or to such class of users as to be effectively available to the public, by or through the operation of any wireless communication device, including any mobile telephone, global positioning system receiving device, mobile computer, or other similar or successor device." S. 1212, §2601(5).

There is also an exception for surveillance conducted for national security purposes. Any agent or officer of the United States is permitted to conduct surveillance as authorized under the Foreign Intelligence Surveillance Act of 1978.

There are two consent provisions in the bill. First, it is not unlawful to intercept geolocation information of a person if that person gives prior consent to such interception. Even if consent is given, however, the information cannot be used for purposes of committing a criminal act in violation of the Constitution or laws of the United States. Second, parents can consent to law enforcement use of the information if a child becomes missing.

In cases of emergency, law enforcement or emergency responders are permitted to use geolocation information to respond to a person requesting assistance (i.e., a 911 call).[155] Also, the police may use this information "in circumstances in which it is reasonable to believe that the life or safety of the person is threatened, to assist the person." If a phone is stolen or taken by fraud, police are permitted to use geolocation information to locate the phone so long as the owner of the phone consents to such use.

Police may use geolocation information if they obtain a warrant in accordance with Federal Rule of Criminal Procedure 41 or as otherwise permitted under the Foreign Intelligence Surveillance Act of 1978. This would codify the practice of federal courts that are currently requiring a warrant based upon probable cause to obtain geolocation information, and would require courts that instead have been relying on the Stored Communications Act's standard of "specific and articulable facts" to follow the majority warrant approach. To permit this change, the act would amend Rule 41 to include geolocation information in the list of items subject to the warrant requirement.

The United States Attorney General and the states' Attorneys General are permitted to intercept geolocation information without a warrant if they (1) reasonably believe that an emergency situation exists, which can include an immediate danger of death or serious physical injury to any person, conspiratorial activities threatening the national security interest, and conspiratorial activities characteristic of organized crime; (2) there are grounds in which an order could be entered to authorize such interception; and (3) an application is then requested within 48 hours after the interception occurs.

The GPS bill contains an exclusionary rule, meaning no evidence acquired in violation of the act may be received in evidence in any trial or other judicial proceeding. This is different from ECPA, which does not contain an exclusionary rule. In addition to this exclusionary remedy, any person whose geolocation information is intercepted may seek civil remedies. The person may seek equitable remedies, damages (money), and reasonable attorneys fees and litigation costs. The damages would be the greatest of (1) whatever the actual damages are to the injured party, and any profits the violator may have made from the violation; (2) $100 a day for each day the entity is in violation of the act; or (3) $10,000. There is a complete defense, however, against any civil and criminal liability if the person believed in good faith that his interception or use of a person's geolocation was permitted under this act. There is also a two-year statute of limitation for such claims. If it is determined that a person willfully or deliberately violated the act, the government is permitted to take disciplinary action against him.

[155] Unlike landline phones in a person's house, the police can only determine a cell phone caller's location either by the caller telling the police where he is located, or by using the geolocation information from the phone.

Section 4 of the GPS bill would amend 18 U.S.C. §1309(h), which criminalizes fraudulently obtaining a person's phone records, to include geolocation information to the types of records subject to this law. Within 180 days after enactment of this act, the United States Sentencing Commission would be required to amend the sentencing guidelines to take into account this revision of §1309.

Conclusion

Congress, the courts, and the people will continue to grapple with "what limits there are upon [the] power of technology to shrink the realm of guaranteed privacy."[156] Some observers believe that ECPA has lived its useful life and should be amended to remain effective. One commentator notes that the "changes in modern technology and shifting security concerns ... result in ambiguous, overlapping guidance in the area of cell phone tracking."[157] Several Members of Congress have introduced legislation to mend this perceived problem, and overhaul the current federal surveillance regime. The Supreme Court has also been asked to weigh in on this debate about the convergence of law and technology in the form of GPS tracking of a person's car. These cases and legislation have the potential to significantly impact the relationship among law, privacy, and technology.

Author Contact Information

Richard M. Thompson
Law Clerk
rthompson@crs.loc.gov, 7-8449

[156] Kyllo v. United States, 533 U.S. 27, 34 (2001).

[157] Kevin McLaughlin, *The Fourth Amendment and Cell Phone Location Tracking: Where are We?*, 29 HASTINGS COMM. & ENT. L. J. 421, 428 (2007).