I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Privacy Implications of GPS Tracking Technology

SARAH RAHTER*

Abstract: Modern advances in Global Positioning System ("GPS") technology have increased the prevalence of GPS-enabled devices in our society. Although these devices provide many valuable services to users, their increasing accuracy and availability has led to decreased privacy in areas previously protected. This note examines the government's collection and use of such technology, along with the impact this use has on an individual's privacy. Additionally, this note explains various viewpoints on the current state of relevant law and advocates the development of clear legal standards to control when the government can invade individuals' privacy by collecting location information about their whereabouts through their GPS-enabled device.

* The author is a 2009 Juris Doctor candidate at The Ohio State University Moritz College of Law. The author has also earned designation as a Certified Information Privacy Professional by the International Association of Privacy Professionals.

I. INTRODUCTION

Global Positioning System ("GPS") technology has come a long way since its inception in 1993.[1] As GPS technology has advanced, it has steadily reduced in size– with some GPS receivers roughly equivalent in size to that of a postage stamp,[2] and price dropping by about 50% in the last few years.[3] As the price and size of GPS receivers have decreased, their accuracy has increased. GPS-enabled surveillance allows a single person to monitor, remotely and simultaneously, the movements of multiple individuals for limitless periods or to determine their precise location at any moment.[4] With recent research reports indicating that by 2012 more than one in ten people will buy a GPS-enabled mobile device each year,[5] it is clear that technological advancements now enable substantial encroachments into zones formerly deemed personal. This infiltration of GPS into our everyday lives has led to concerns regarding the level of privacy that individuals can expect when using GPS devices.

Currently, no legislation exists to restrict the government's collection or use of GPS tracking information against suspected criminals, and only a few states have enacted legislation that restricts the commercial use of GPS. [6] Absent legislation, the Fourth Amendment acts as the only federal limit to the government's use of such technology. However, its protection of individuals from

---

[1] For a closer look into the origin of the Global Positioning System and the advancement of GPS technology, see Kevin Keener, *Personal Privacy in the Face of Government Use of GPS*, 3 ISJLP 473, 474 (2007).

[2] James Klein, *Brave New GPS World*, Nov. 3, 2003, GTX CORP., http://gtxcorp.com/?q=/news/in_the_news.

[3] Charles Murray, *GPS Makers Lock on to Personal Security Technology*, EETIMES.COM, Aug. 15, 2002, http://www.eetimes.com/story/OEG20020815S0051.

[4] *See infra* Parts I.A and I.B for a full discussion of the functioning of GPS systems used for enhanced surveillance.

[5] To purchase the complete report, see HARRY WANG, GPS: A PATH TO NEW APPLICATION ON MOBILE DEVICES (May 2008), http://parksassociates.ecnext.com/coms2/summary_0256-9984_ITM; *see also, GPS-integrated Mobile Devices Head for Ubiquity*, GIZMAG, June 9, 2008, at 1, *available at* http://www.gizmag.com/gps-integrated-mobile-devices-head-for-ubiquity/9443/.

[6] CONN. GEN. STAT. § 42a-9-609 (2003); CAL. CIV. CODE § 1936(6)(o) (2002); N.Y. GEN. BUS. LAW § 20 Art. 26 § 396-z (2006).

unreasonable search and seizure has become less effective in our society, where technological advancements operate to reduce the individual's reasonable expectation of privacy in public.[7]

New technology enables unprecedented government access into particularized activities and locations of individuals. Unfortunately, government efforts to establish policies to protect the individual's right to privacy lag behind these technological advancements. With little legislative guidance, it remains unclear what level of individual privacy the law is prepared to recognize in a society permeated by technology.

This note considers what limits the Constitution, federal and state statutes, and current case law impose on government use of GPS and other tracking technology. Part I of this article examines the capabilities of vehicular GPS and the privacy implications associated with government use of such technology. Part II presents the privacy implications of cellular phones with tracking technologies and the current regulation limiting the government's access to information transmitted through and stored by cellular service providers. Part III examines the academic perspective on government use of GPS technology and the contention that the Fourth Amendment affords greater protection for individuals against government intrusion than current law provides.

II. IN-CAR NAVIGATION

"Of the new vehicles currently on the road, fifteen percent are equipped with [GPS devices]."[8] Telematics refers to automobiles receiving remote information from commercial service providers, including such services as Global Positioning System ("GPS"), on-demand entertainment, Internet and Web access, or weather and traffic conditions.[9] "With more than two million subscribers and fifty

---

[7] The Supreme Court has shown reluctance in restricting the efficient collection of information through technological means, where that information could permissibly be collected through traditional means. *See, e.g.*, Katz v. United States, 389 U.S. 347, 351 (1967); United States v. Knotts, 460 U.S. 276, 282 (1983); *but see* Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that government surveillance using devices not in general public use to obtain information about the interior of the home was a search considered "presumptively unreasonable without a warrant").

[8] *GPS Steering You in the Wrong Direction?*, ABC NEWS, Jan. 15, 2008, http://abcnews.go.com/GMA/Consumer/story?id=4136269.

[9] Cherise Fong, *What is Telematics?*, CNN.COM, Jan. 3, 2008, http://www.cnn.com/2007/TECH/12/20/skorea.telematics/index.html#cnnSTCText.

GM OnStar-enabled vehicles, OnStar is the leading provider of telematics services in the United States."[10] OnStar offers a list of services including everything from turn-by-turn navigation, stolen vehicle location, and AccidentAssist to remotely unlock doors or turn on the vehicle's horn and lights.[11]

Vehicles without factory-installed GPS may utilize new Personal Navigation Devices ("PNDs") for in-car navigation. PNDs come in many varieties and provide almost the same functionality as in-car navigation systems, but at a fraction of the cost. Some PNDs can monitor vehicles through a small box plugged into a car dashboard, allowing the remote download of data from the box, including the car's location and speed, onto computers.[12] Others deliver GPS real-time tracking information covertly by magnetically attaching to the car's undercarriage.[13] The proliferation of GPS vehicle navigation raises concerns about encroachments on individual privacy as third parties access vehicle-tracking information. The following section outlines current federal and state regulation relating to government installation and use of GPS vehicle tracking.

A. FEDERAL REGULATION OF TECHNOLOGY

On December 1, 2006, Rule 41 of the Federal Rules of Criminal Procedure was amended to set forth procedures for federal agents to obtain, process, and return warrants for installation and use of tracking devices.[14] Unfortunately, neither the amended Rule 41, nor the tracking-device statute[15] specifies the standard an applicant must

---

[10] OnStar, OnStar Technology, http://www.onstar.com/us_english/jsp/explore/onstar_basics/technology.jsp (last visited Jan. 17, 2009).

[11] OnStar, Onstar Services, http://www.onstar.com/us_english/jsp/explore/onstar_basics/services.jsp (last visited Jan. 17, 2009).

[12] *GPS Technology Helps Parents Track Teens*, NEWSHOUR EXTRA, Feb. 19, 2007, http://www.pbs.org/newshour/extra/features/jan-june07/gps_2-19.pdf.

[13] *GPS Tracking Key*, GPS TRACKING REVIEW.COM, Apr. 4, 2008, http://www.gpstrackingreview.com/2008/04/gps-tracking-key/.

[14] *See* FED. R. CRIM. P. 41.

[15] The purpose of 18 U.S.C. § 3117, also referred to as the "Tracking Device Statute," is to provide a court with extra-territorial jurisdiction over use of tracking devices installed within its jurisdiction. This provision does not itself affirmatively require that the

meet to install a tracking device.[16] Absent concrete legislative protection from GPS tracking, individuals have challenged such tracking as an unreasonable search or seizure under the Fourth Amendment.

While the Fourth Amendment does not provide a general constitutional right to privacy, it does protect citizens from any government intrusions that constitute unreasonable searches and seizure.[17] Different standards have evolved to describe the level of proof that law enforcement must have before conducting a legally permissible search of a person or property. Probable cause is the highest standard, which must be met to procure a warrant, while a showing of clear and articulable facts establishes the lesser showing of reasonable suspicion.[18] The Supreme Court created the presumption that police must secure a warrant prior to conducting a search of a suspect, absent exigent circumstances.[19] Thus, the central issue in GPS tracking cases is whether the use of the GPS device constitutes a search. If it does, than it follows that police must secure a warrant prior to using a GPS device to track a suspect, absent exigent circumstances. If a court, however, finds that government use of a GPS device is not a search under the Fourth Amendment, then no warrant is necessary and the Fourth Amendment requires a lower burden of proof on the part of the government before allowing them to track suspects using GPS.

While the Supreme Court has not yet decided whether the installation of a GPS tracking device constitutes a search under the Fourth Amendment, it has established the general limitations on

---

government obtain such a warrant or other order, or otherwise define the standards under which the use of a tracking device may be authorized. *See* In the Matter of the Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 534 F. Supp. 2d 585, 593, 595 (W.D. Pa 2008) (noting that the Tracking Device Statute does not specify the evidentiary standard applicable to the installation of a tracking device).

[16] 18 U.S.C. § 3117 (2008).

[17] *Katz*, 389 U.S. at 350.

[18] Different standards apply for national security surveillance. For a discussion of these standards, see generally Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GWLR 1306 (2004).

[19] United States v. Leon, 468 U.S. 897, 913 (1984); Mincey v. Arizona, 437 U.S. 385, 390 (1978).

government use of tracking technology through case law.[20] *Katz v. United States* was the first case in which the Court determined that "what a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[21] In *United States v. Knotts,* the Court determined that the warrantless tracking of a beeper did not constitute a violation of the defendant's Fourth Amendment right,[22] reasoning, "a person traveling in an automobile . . . has no reasonable expectation of privacy in his movement from one place to another."[23]

Referencing the *Knotts*[24] decision, a district court in *United States v. Eberle* stated that "use of a radio transmitter to monitor an automobile's progress on public roads is not a search within the meaning of the Fourth Amendment."[25] The next year, in *United States v. McIver*, the Ninth Circuit held that the defendant did not have an expectation of privacy in the undercarriage of his truck and that the defendant did not demonstrate that he intended to shield the undercarriage from inspection by others.[26] Therefore, the attachment and use of a GPS device by the police was not an unreasonable search under the Fourth Amendment.[27] The court further determined that the placement of the GPS was not a seizure within the meaning of the Fourth Amendment as there was no evidence that the device deprived defendant of dominion and control over his vehicle or that the presence of the device caused damage to the vehicle's electronic components.[28] Nonetheless, courts have disallowed routine government surveillance where such surveillance cannot be completed with "a minimum of interference" with the in-car navigation system.[29]

---

[20] For a discussion on the evolution of Supreme Court case law on the subject of government use of tracking technology see Keener, *supra* note 1, at 476.

[21] *Katz*, 389 U.S. at 351.

[22] *Knotts*, 460 U.S. at 276.

[23] *Id.* at 281.

[24] *Id.* at 276.

[25] United States v. Eberle, 993 F. Supp. 794, 798 (D. Mont. 1998).

[26] United States v. McIver, 186 F.3d 1119, 1127 (9th Cir. 1999).

[27] *Id.*

[28] *Id.*

[29] Company v. United States (*In re United States*), 349 F.3d 1132, 1144 (9th Cir. 2003) (ultimately finding in-car navigation service provider not required to commence cellular

As of this writing, the most recent federal case that determined the constitutionality of warrantless installation and use of GPS by the government to track a suspect's vehicle was *U.S. v. Moran.*[30] Equating GPS tracking with visual surveillance, the court held that the warrantless use of GPS by police to track Moran was permissible under the Fourth Amendment because, "Moran had no expectation of privacy in the whereabouts of his vehicle on a public roadway."[31] However, as the log and recording functions of GPS devices progress—providing far more detailed records than visual surveillance could ever have provided—the same rule continues to be applied by federal courts, and accordingly, what is out in the open can be tracked by technology. The exception to this rule of permissibility is instances where surveillance by law enforcement goes beyond a "minimum of interference" with the GPS system.

In *Company v. United States* (In re United States), the Court addressed when a company, not a common carrier, possessing the ability to facilitate the interception of oral communications, may be required to assist law enforcement in intercepting such communications.[32] In this case, court orders required the company to assist the FBI in eavesdropping on conversations occurring inside a vehicle equipped with a GPS system.[33] The Court held that if the company was both a "provider of wire or electronic communication service" and an "other person" within the meaning of 18 U.S.C. § 2518(4), it could be required to furnish facilities and technical assistance.[34] However, the Court also noted that "court orders granted pursuant to the authority of § 2518 must specify that assistance be provided 'unobtrusively and with a minimum of interference with the services that such service provider, landlord . . . or person is according the person whose communications are to be intercepted.'"[35] In

---

connection function of vehicle to enable FBI eavesdropping on oral communications within the car because the FBI's use of the passive listening feature disabled other system services, and therefore, the surveillance could not be completed with "a minimum of interference" with the system's operation as required under 18 U.S.C. § 2518(4) wiretap law).

[30] *See* United States v. Moran, 349 F. Supp. 2d 425, 432 (N.D.N.Y 2005).

[31] *Id.* at 467.

[32] *Company*, 349 U.S. at 1137.

[33] *Id.*

[34] *Id.* at 1144.

[35] *Id.*

Company, the Court held that because FBI surveillance completely disabled the monitored car's GPS system, and severely hampered the emergency features of the car, Company was not required to assist the FBI in interception of the phone conversations because it could not be done with "a minimum of interference" with the service provided by Company, as required by 18 U.S.C. § 2518(4).[36]

In addition to protecting citizens from government surveillance that interferes with their GPS systems, federal case law also places Fourth Amendment restrictions on the government's use of GPS where such use intrudes upon the suspect's home or curtilage thereof.[37] The home exception to otherwise lawful technologically enhanced searches is well established.[38] Following the establishment of this exception, the Supreme Court in *Kyllo v. United States* held that the government's use of a thermal-imaging device constituted a search in violation of the defendant's Fourth Amendment right and that government use of surveillance devices not in general public use, to obtain information about the interior of the home, is a search considered "presumptively unreasonable without a warrant."[39] Thus, these federal cases suggest that government use of GPS technologies to track suspects without a warrant is legally permissible so long as the surveillance is conducted outside the home or curtilage thereof, with widely available technology, and does not result in more than a minimum of interference into the tracked object's system operation.

---

[36] *Id.* at 1146.

[37] *See* Oliver v. United States, 466 U.S. 170, 180 (1984) (curtilage encompasses area "immediately surrounding and associated with the home . . . to which extends the intimate activity associated with the 'sanctity of a man's home and the privacies of life'").

[38] *See* Silverman v. United States, 365 U.S. 505, 509 (1961) (warrantless police intrusion into defendant's home violates the Fourth Amendment even if the information thus collected could have been obtained by other means); *see also* United States v. Moore, 562 F.2d 106, 114 (1st Cir. 1977) (warrantless use of a beeper inside a box of chemicals to determine their continued presence in the residence infringed on defendants' Fourth Amendment rights); *see also* United States v. Karo, 468 U.S. 705, 714 (1984) (monitoring a beeper becomes a search under the Fourth Amendment when it reveals "a critical fact about the interior" of a home); *see also Oliver*, 466 U.S. at 176–78 (holding that individuals "may not legitimately demand privacy for activities conducted out of doors in fields, except in the area immediately surrounding the home").

[39] *Kyllo*, 533 U.S. at 40.

B. STATE REGULATION OF TECHNOLOGY

While federal law permits the warrantless attachment of an electronic monitoring device to the exterior of a person's vehicle, "states are free to interpret their own constitutional provisions as providing greater protections than analogous federal provisions."[40] A few states—Alaska, Florida, Hawaii, and Illinois—have amended their constitutions to include express provisions protecting their citizens against government invasions of privacy, including those perpetrated through the use of electronic surveillance.[41] State courts remain split over the use of GPS tracking devices by law enforcement, with some following the federal model and others requiring warrants before allowing installation of such devices.

1. STATES WHERE NO WARRANT IS REQUIRED

In California, Nevada, and Wisconsin, law enforcement agents do not need to obtain a warrant before using GPS technology to track a suspect.[42] A California Appeals Court ruled that no warrant is necessary where police attach a GPS monitor to the outside of a vehicle and monitor its signals while traveling.[43] The court held police examination of the undercarriage of a vehicle—to touch it, or to attach a tracking device to it—does not amount to a search under the Fourth Amendment, "so long as a police officer does so from a place where

---

[40] Osburn v. State, 118 Nev. 323, 325 (2002) (citing Michigan v. Long, 463 U.S. 1032, 1041 (1983)).

[41] The Illinois Constitution provides, "The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means. No warrant shall issue without probable cause, supported by affidavit particularly describing the place to be searched and the persons or things to be seized." ILL. CONST. art. 1, § 6. Similarly, the Hawaiian Constitution states, "The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest." HAW. CONST. art. 1, § 6. Likewise, the Alaskan Constitution states, "The right of the people to privacy is recognized and shall not be infringed." ALASKA CONST. art. I, § 22. Finally, the Florida Constitution states, "Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein." FLA. CONST. art. 1 § 23.

[42] For an in-depth analysis of the progression of state law regarding government tracking through GPS technologies, see Keener, *supra* note 1, at 481.

[43] People v. Zichwic, 94 Cal. App. 4th 944 (6th Dist. 2001).

the officer has a right to be."[44] Similarly, the Supreme Court of Nevada concluded that police use of a monitoring device attached to defendant's vehicle without a warrant did not constitute an unreasonable search because the defendant had neither a subjective nor an objective expectation of privacy in the bumper of his vehicle.[45]

Most recently, the Court of Appeals for the Seventh Circuit in Wisconsin held in *United States v. Garcia* that police placement and use of a GPS tracking unit attached to the defendant's car did not constitute a search or seizure within the meaning of the Fourth Amendment.[46] In *Garcia*, police suspected the defendant was involved in the manufacturing of methamphetamines, so they installed a GPS device to the defendant's vehicle while the car was parked on a public street.[47] After reviewing the information obtained from the GPS device, police obtained a warrant and after searching the locations where the vehicle had been driven, found materials used to manufacture methamphetamines.[48] Accordingly, defendant was charged "with crimes relating to the manufacture of methamphetamine."[49] Stating that "[t]here is a tradeoff between security and privacy, and often it favors security,"[50] Judge Posner, as author of the opinion, denied the defendant's request to suppress evidence obtained from the tracking device as fruit of an unconstitutional search.[51] In his decision, Posner noted that the advancement of technology enables an evisceration of privacy and allows for "an extent of surveillance that in earlier times would have been prohibitively expensive."[52] He did not, however, resolve the issue by endorsing or dismissing the dangers of mass surveillance. Instead, he notes that "[s]hould government someday decide to institute programs of mass surveillance of vehicular movements, it

---

[44] *Id.* at 956.

[45] *Osburn*, 118 Nev. at 327.

[46] United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

[47] *Id.* at 995.

[48] *Id.*

[49] *Id.*

[50] *Id.* at 998.

[51] *Id.* at 997.

[52] *Id.* at 998.

will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search."[53]

2. STATES WHERE A WARRANT IS REQUIRED

In contrast to California, Nevada, and Wisconsin, warrants are required in Oregon, Washington, and Louisiana under state law before police may employ vehicle-tracking transmitters.[54] The courts in Oregon, Washington, and Louisiana all found that police use of a tracking device was a particularly intrusive method of surveillance and, as such, required police to obtain a warrant before using such technology, in the absence of an obviating exigency.[55] In these states, any warrantless use of GPS tracking technology is presumptively unreasonable and it follows that any evidence obtained through such a search will be excluded in the courts of these states as the fruits of an unconstitutional search.

3. A STATE WITH CONFLICTING CASE LAW

In New York, two courts of equal authority have considered the issue, reaching conflicting conclusions. The Nassau County Court held in *People v. Lacey* that installation of GPS on a car reportedly used in a string of burglaries fell within both federal and New York constitutional protections against warrantless searches and seizures.[56] The court emphasized the explicit protection provided by Article 1,

---

[53] *Id.*

[54] For a thorough examination of the progression of state law in this area, see Keener, *supra* note 1, at 481.

[55] *See* State v. Campbell, 759 P.2d 1040, 1047 (Or. 1988) (while the text of the Oregon law and the federal Constitution are similar, the Oregon Supreme Court construed their state Constitution more broadly by holding that "a privacy interest . . . is an interest in freedom from particular forms of scrutiny"); *see also* State v. Jackson, 150 Wash.2d 251, 264 (Wash. 2003) (finding that "[u]se of GPS tracking devices is a particularly intrusive method of surveillance, making it possible to acquire an enormous amount of personal information about citizens under circumstances where the individual is unaware that every single vehicle trip taken and the duration of every stop may be recorded by the government); State v. Peters, 546 So. 2d 829, 834 (La. App. 1 Cir. 1989) (noting that police had guarded against any Fourth Amendment violation by obtaining a warrant prior to attaching a beeper to defendant's car).

[56] People v. Lacey, No. 50358U, slip. op. at 1 (N.Y.S.2d May 6, 2004).

§ 12 of the New York Constitution that extends Fourth Amendment protection against unreasonable searches and seizures to telephone and telegraph communications, reasoning that the same protection should extend to the installation of a GPS device.[57] In the opinion, Judge Calabrese acknowledged that persons have diminished expectations of privacy in automobiles on public roads, but stressed that "the mere act of parking a vehicle on a public street does not give law enforcement the unfettered right to tamper with the vehicle by surreptitiously attaching a tracking device."[58]

In contrast, the New York County Court for Westchester County agreed with the *Moran* District Court for the Northern District of New York, holding that police did not need a warrant prior to attaching a GPS unit to defendant's RV.[59] Since defendant did not own the vehicle and had no legitimate expectation of privacy in its movements on public roads, the court found he had no privacy expectation sufficient to establish standing to challenge use of the GPS device within the purview of the Fourth Amendment.[60] The court went on to find that "no greater privacy interest is afforded to a vehicle traveling upon a public roadway under the New York State Constitution than that which is afforded under the United States Constitution."[61] The court went further, stating that, "there is no reasonable expectation of privacy in the movements of a motor vehicle traveling upon public roadways such that law enforcement is required to obtain a warrant under New York state law prior to installing a GPS device when investigating crime."[62]

This split leaves the future unclear for prospective challenges to New York law enforcement's warrantless use of GPS technology. However, in considering the *Gant* and *Moran* holdings together, it seems the New York Constitution does not require law enforcement to obtain a warrant.[63]

---

[57] *Id.* at 5.

[58] *Id.* at 8.

[59] People v. Gant, No. 25307, slip op. at 3–5 (N.Y.S.2d July 27, 2005).

[60] *Id.* at 845–46.

[61] *Id.* at 847–48.

[62] *Id.*

[63] Relying on *Knotts*, both courts determined that the defendant had not established a legitimate expectation of privacy in a vehicle traveling upon a public roadway such that law enforcement was required to obtain a search warrant prior to its installation of a GPS

III. CELLULAR COMMUNICATIONS AND STORED RECORDS

The following section examines the privacy implications associated with the use of cellular phones integrated with tracking technologies and the current regulation on the government's access to information transmitted through such cellular phones and stored by service providers. For a cellular phone to receive calls there must be continuous communication between the physical phone and the carrier's satellite towers.[64] This signal communication can be used by carriers to track the whereabouts of individuals by triangulating the signal (measuring the relative time delays in the signal from the phone to three different base stations).[65] Developing technology coupled with an increasing number of cell sites built to handle the rapidly expanding cell phone market have led to increased accuracy in triangulating the physical location of a user.

The push for increased accuracy in triangulating the physical location of a user was prompted by the Federal Communications Commission and supported by many professional organizations as a means of aiding emergency services.[66] Government response came through a federal regulation aimed at enhancing 911 Service.[67] The regulation requires service providers to "achieve 95 percent penetration of location-capable handsets among its subscribers."[68] Traditionally, cellular carriers have averaged their compliance with FCC rules over an entire state or multi-state region, but the FCC announced new rules on September 11, 2007, requiring operators to meet FCC requirements within every 911 calling area by 2012.[69] As

---

device to track the vehicle's whereabouts. *See Gant*, No. 25307, slip op. at 846; *Moran*, 349 F. Supp. 2d at 467.

[64] OFFICE OF TECH. ASSESSMENT, WIRELESS TECHNOLOGIES AND THE NATIONAL INFORMATION INFRASTRUCTURE 81 (1995), http://www.princeton.edu/~ota/disk1/1995/9547/954706.PDF.

[65] *Id.* at 98.

[66] Darren Handler, *An Island of Chaos Surrounded by a Sea of Confusion: The E911 Wireless Device Location Initiative*, 10 VA. J.L. & TECH. 1, 5 (2005) (discussing the evolution of 911 and GPS triangulation to locate wireless callers).

[67] 47 C.F.R. § 20.18 (2006).

[68] *Id.*

[69] Marguerite Reardon, *FCC Mandates More Stringent E911 Compliance*, CNET NEWS.COM, Sept. 12, 2007, http://www.news.com/FCC-mandates-more-stringent-E911-compliance/2100-1039_3-6207530.html.

technology builds, so do concerns about the privacy implications of such technology, with many people fearing government misuse of the staggering amount of data collected by service providers. The following section examines the numerous legal standards that courts have adopted for government access to information and how those legal standards affect regulation of government surveillance. In addition, the differing positions of the Department of Justice and the Electronic Frontier Foundation regarding what standard should apply to such government surveillance will be examined.

A. OVERVIEW OF LEGAL STANDARDS FOR GOVERNMENT ACCESS OF COMMUNICATIONS AND STORED DATA[70]

Privacy law has not kept pace with emerging technology. Thus far, court cases contemplating new technologies have been inconclusive or inconsistent in their holdings, offering few clear restrictions on government surveillance. As courts and legislators have grappled with various technologies, multiple legal standards have emerged for government access to information. The law seems clear in the area of stored data: the government is able to access any collected information from a third party with only a subpoena if the records are likely to lead to relevant evidence and this access will not violate the Fourth Amendment.[71] In all other areas, a sliding scale of legal standards exists with different standards applying to different information, depending on the sensitivity of the information.[72] Since no statute delineates precise standards for government location tracking, the recurring question for courts and legislatures is which of these standards to apply to emerging technologies.

---

[70] For an explanation of background case law relating to government tracking of cellular phones and government access to stored records regarding location, see Keener, *supra* note 1, at 489–95.

[71] *See* United States v. Miller, 425 U.S. 435, 443 (1976) (Where information was voluntarily conveyed to a third-party bank, the Court held that the defendant took "the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government.").

[72] The Center for Democracy and Technology provides a chart outlining what information the government can get and what standard must be met to obtain that information. According to the chart, law enforcement's real-time interception of dialed numbers by pen register/trap and trace devices are not subject to a showing of probable cause. *See* Ctr. for Dem. & Tech., *Current Legal Standards for Access to Papers, Records, and Communications: What Information Can the Government Get About You, and How Can They Get It*, July 2006, www.cdt.org/wiretap/govaccess/govaccesschart-11x17.pdf.

1. PROBABLE CAUSE

As summarized in Part I.A of this note, with some distinguished exceptions, a search is only reasonable under the Fourth Amendment if carried out pursuant to a warrant. Warrants are issued by a judge based on a finding of probable cause to believe that a crime either is being, has been, or is about to be committed and that the search will lead to evidence of the crime.[73] In essence, all the government must show to prove probable cause is that a reasonably prudent person would believe that the search of a particular area will produce evidence of a crime given the totality of the circumstances.[74]

2. PROBABLE CAUSE PLUS

In the *Katz* and *Berger* cases, the Supreme Court held that the Fourth Amendment protects the content of telephone calls and face-to-face conversations.[75] Congress responded to the Court's decisions in the *Katz* and *Berger* cases by adopting the "Wiretap Act" that set procedures for court authorization of real-time surveillance of all kinds of electronic communications, including voice, e-mail, fax, and Internet, in criminal investigations.[76] The Act normally requires that a judge issue an order, based on an affidavit provided by the government, that there is probable cause to believe that a crime has been, is being, or is about to be committed *before* a wiretap can commence.[77]

---

[73] James Dempsey, *Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology*, 935 PLI/PAT 543, 552 (2008).

[74] *Garcia*, 474 F.3d at 996.

[75] *Katz*, 389 U.S. at 352 (holding that government interception of telephone calls constitutes a search and seizure under the Fourth Amendment); *see also* Berger v. New York, 388 U.S. 41 (1967) (suggesting that the uniquely intrusive aspects of wiretaps required procedural protections beyond those provided by a basic search warrant).

[76] 18 U.S.C. § 2510–2522 (2006) (a 1968 statute discussing telecommunications).

[77] *Id. See also* Ctr. for Dem. & Tech., *The Nature and Scope of Governmental Electronic Surveillance Activity*, July, 2006, http://www.cdt.org/wiretap/wiretap_overview.html.

3. REASONABLE SUSPICION BASED ON "SPECIFIC AND ARTICULABLE FACTS"

Reasonable suspicion requires a lower burden of proof than obtaining a warrant and probable cause. Where the burden is reasonable suspicion, police may obtain cell site information upon a presentation of "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." [78] Congress's decision to leave the Pen/Trap Statute unchanged has resulted in a higher standard of protection for transactional data in storage than for transactional data in transit. [79] In jurisdictions requiring probable cause, a search warrant issued by the court is the only document compelling company disclosure of real-time tracking information to law enforcement. Therefore, in jurisdictions requiring probable cause, companies must only release information where law enforcement serves upon them a valid search warrant based on the high standard of probable cause.

4. LESS THAN REASONABLE SUSPICION

In 1979, the Supreme Court ruled that individuals have no reasonable expectation of privacy in digits dialed from one's home phone.[80] Therefore, installation and use of a pen register (a record of outgoing calls from a particular number) or trap and trace (a record of incoming calls to a particular number) by the police is not a search. To obtain a pen register or trap and trace device order (Pen/Trap), the government only needs to show that "the information likely to be obtained is relevant to an ongoing criminal investigation."[81] A judge must approve any government request for a Pen/Trap upon a mere certification of relevance, a drastically decreased standard than the probable cause standard required for searches under the Fourth Amendment.[82] However, if the government only obtains a court order

---

[78] 18 U.S.C. § 2703(d) (2006).

[79] Dempsey, *supra* note 73, at 555.

[80] Smith v. Maryland, 442 U.S. 735, 738 (1979).

[81] 18 U.S.C. § 3122(b)(2) (2006).

[82] 18 U.S.C. § 3123(a)(1) (2006).

for a Pen/Trap, "call identifying information"[83] should not include "any information that may disclose the physical location of the subscriber."[84] Therefore, government agents that only obtain a court order for a Pen/Trap may only obtain the general cell site location information from the communications carrier.

B. OPPOSING VIEWPOINTS ON CURRENT LEGAL STANDARDS

The specific issue of whether real-time cell site information requires a higher burden than that of pen register information (a record of outgoing calls from a particular number) or trap and trace information (a record of incoming calls to a particular number) has been decided in fewer than twenty courts across the United States. In these cases, the government alleges that the Pen/Trap Statute and the Stored Communications Act ("SCA"), which forbid disclosure of cell site information "solely pursuant" to a Pen/Trap order,[85] allow disclosure of cell site information pursuant to an "articulable facts" order issued under 18 U.S.C. § 2703(d). This argument, often referred to as the hybrid theory, asserts that by working pursuant to both the SCA and the Pen/Trap statute, the government has the right to obtain cell site information without probable cause or a search warrant. Traditionally, judges have not held law enforcement officials to a high burden when issuing phone warrants, but groups like the American Civil Liberties Union ("ACLU") and the Electronic Frontier Foundation ("EFF") have fought the Department of Justice ("DOJ") for over a decade to ensure that the courts hold law enforcement to a higher burden of proof prior to issuing a phone warrant.

While the DOJ regularly obtains court orders or warrants in order to collect telephone data, the government has increasingly participated in wiretapping without first obtaining warrants since September 11, 2001. The DOJ claims that "[w]arrantless eavesdropping on calls between people in this country and suspected terrorists overseas is a legal and 'indispensable' part of safeguarding the nation against future attacks" and that the practice does not

---

[83] Call identifying information is defined by the Communications Assistance for Law Enforcement Act of 1994 as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." 47 U.S.C. § 1002(a)(2)(A) (2006).

[84] 47 U.S.C. § 1002(a)(2)(B) (2006).

[85] *See id.*

violate constitutionally protected civil liberties.[86] In addition to tapping phone lines, the DOJ began requesting that they be allowed to gather real-time location data of cellular telephones along with Pen/Trap orders. The ACLU and the EFF have continually challenged the DOJ's requests for real-time cell phone tracking information, arguing that real-time tracking is "invasive" and poses such a threat to privacy that the DOJ should be required to show probable cause before obtaining a warrant to obtain such information.[87]

A majority of the courts denied the government's requests, concluding that, "statutory authority for prospective cell site location information is lacking."[88] These courts were not convinced that the SCA refers to real-time data or that the Pen/Trap statute gives a right to information tracking a user's location. Under this approach, the only way to grant the government access to such information is under Federal Rule of Criminal Procedure 41(d)(1), which requires a showing of probable cause before a search warrant is issued.[89] Currently, only two judges—both from the Southern District of New York—have dissented from the majority position, adopting a broad interpretation of the PATRIOT Act's expansion of the definition of

---

[86] Humphrey Cheung, *EFF Battles DOJ on Real-time Cell Phone Tracking*, TG DAILY, Oct. 27, 2005, at 1, *available at* http://www.tgdaily.com/content/view/21217/118/.

[87] *Id.*

[88] In re App. of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 2006 WL 468300, *1 (S.D.N.Y.); *see* In re Matter of App. for an Order Auth. the Installation and use of a Pen Register and Directing the Disclosure of Telecomms. Records for the Cell Phone assigned the No. [Sealed], 439 F. Supp. 2d 456, 457 (D.Md. 2006); In re of the Application of the U.S. for an Order Auth. (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking, 441 F. Supp. 2d 816 (S.D. Tex. 2006); In re App. of the U.S. for an Order (1) Auth. the Installation and Use of a Pen Register and Trap and Trace Device (2) Auth. the Release of Subscriber and Other Info. and (3) Auth. the Disclosure of Location-Based Servs., 2006 WL 1876847 (N.D.Ind.); In re App. of the U.S. for Orders Auth. the Disclosure of Cell Cite Info., 2005 WL 3658531 (D.D.C.); In re App. of the U.S. for Orders Auth. the Install. and Use of Pen Registers and Caller Identification Devices on Tel. Nos. [Sealed], 416 F. Supp. 2d 390 (D.Md. 2006); In re App. of the U.S. for an Order Auth. Installation and Use of a Pen Register and/or Trap and Trace and the Disclosure of Subscriber and Activity Info., 415 F. Supp. 2d 211 (W.D.N.Y. 2006); In re App. of the U.S. for an Order Auth. the Release of Prospective Cell Site Info., 407 F. Supp. 2d 134 (D.D.C. 2006); Wisconsin Decision, 412 F. Supp. 2d at 947, 949 (2006); E.D.N.Y. Decision, 396 F.Supp.2d 294, 295 (2005); Maryland I Decision, 402 F. Supp. 2d 597, 605 (2005); Texas Magistrate Decision, 396 F. Supp. 2d 747, 765 (2005).

[89] *See* In re App. of the U.S. for an Order Auth. the Use of a Pen Register and a Trap Device, 396 F. Supp. 2d. 294, 321 (E.D.N.Y. 2005).

"pen register,"[90] and holding that the Communications Assistance for Law Enforcement Act ("CALEA")[91] requires use of an additional authority when ordering disclosure of prospective cell site information. These courts have rejected the majority position–deciding that the SCA provides the additional statutory authority required under CALEA.[92]

While government access to third-party stored records requires only a subpoena for records containing relevant location information,[93] law enforcement's use of cellular real-time tracking faces different rules in different jurisdictions. In the minority of jurisdictions, police may obtain cell site information upon a showing of "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."[94] In jurisdictions requiring probable cause, a search warrant issued by the court is the only document compelling company disclosure of real-time tracking information to law enforcement. Therefore, companies in the listed jurisdictions must release any information requested by a valid search warrant served upon them. However, companies remaining outside these jurisdictions may be compelled to release information upon a lesser standard than probable cause.

IV. ACADEMIC PERSPECTIVE ON PRIVACY AND THE FOURTH AMENDMENT

Courts to date have generally held that individuals have waived their right to privacy when in public, and thus, there are few barriers to GPS tracking. In a new book challenging this status quo, however, legal scholar Christopher Slobogin, has suggested an alternative approach that would apply stricter Fourth Amendment protections. In *Privacy at Risk: The New Government Surveillance and the*

---

[90] Finding that the term "signaling information" added by the USA PATRIOT Act in 2001 includes cell phones since they emit signal information. *See* Pub.L. No. 107-56, § 216(c)(2), 115 Stat. 272, 290 (2001).

[91] 47 U.S.C. § 1001 et seq. (2006).

[92] 18 U.S.C. § 2701 et seq. (2006).

[93] *See* FED. R. CIV. P. 26(b).

[94] 18 U.S.C. § 2703(d) (2006).

Fourth Amendment, Slobogin examines the government's use of surveillance and how new surveillance technologies are allowing the government to subvert the privacy protections of the Fourth Amendment.[95]

Slobogin contends that, while government use of surveillance is a potent law enforcement tool, it represents an insidious assault on the freedom of Americans and should be subject to meaningful regulation, which current law fails to provide.[96] He asserts that, "[t]he assault comes from government monitoring of our communications, actions, and transactions. The failure results from the inability or unwillingness of courts and legislatures to recognize how pervasive and routine this government surveillance has become."[97] Slobogin insists that Americans have a right to public anonymity and to preserve this right, the judicial decisions outlined in Parts I and II of this article need to be reversed or reinterpreted to permit much more significant regulation of government use of surveillance. In his own words: "This book is meant to prod legislatures and courts into more meaningful constraints on physical and transaction surveillance." Slobogin states that existing government surveillance techniques "[i]n their current minimally regulated state . . . do real harm to individual interests and ultimately to society and government itself. That state of affairs must change."[98]

Expanding a framework developed by the Supreme Court almost forty years ago in *Terry v. Ohio,* [99] Slobogin proposes the proportionality principle to replace the current Fourth Amendment framework used by the courts. The proportionality principle advocates that when contemplating surveillance, courts should require the government to provide justification proportionate to the intrusiveness of the surveillance, and in all non-exigent circumstances, the government should be required to seek third-party authorization.[100] Slobogin explains[101] that his approach to the Fourth

---

[95] CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 1 (The University of Chicago Press 2007).

[96] *Id.* at 5.

[97] *Id.* at viiii.

[98] *Id.* at x.

[99] 392 U.S. 1 (1968).

[100] SLOBOGIN, *supra* note 95, at 21.

Amendment and its application to surveillance are largely an elaboration of the principle in *Terry* that, "[t]here is 'no ready test for determining reasonableness other than by balancing the need to search (or seize) against the invasion which the search (or seizure) entails.'"[102]

In order to employ the proportionality analysis proposed by Slobogin, courts must first establish a hierarchy of invasiveness in order to gauge the relative intrusiveness of a police action that is considered a search or a seizure.[103] Slobogin asserts that the appropriate reference point for evaluating the relative invasiveness of different government surveillance techniques should include some assessment of societal attitudes and, thus, courts should begin with the *Katz* declaration that the Fourth Amendment protects only expectations of privacy that "society is prepared to recognize as reasonable,"[104] and as a second step, determine when a particular government intrusion is justified. To determine this, Slobogin suggests a four tier hierarchy that would apply across the board to all searches and seizures.[105] Slobogin asserts that the two levels of current justification, probable cause and reasonable suspicion, are insufficient. To bolster the effectiveness of Fourth Amendment scrutiny, he adds a standard of clear and convincing proof, as well as a relevance standard to his proposed hierarchy. As described by Slobogin, the revised hierarchy would consist of: (1) clear and convincing proof: government must show clear and convincing proof that the evidence sought is crucial to the state's case (75% level of certainty); (2) probable cause: equated with a more-likely-than-not finding or possibly a level of certainty slightly below that (51% level of certainty); (3) reasonable suspicion: relaxation of the probable cause standard (30% level of certainty); and (4) relevance standard: some articulable reason for believing government action has some tendency to lead to information helpful to solving a crime or apprehending a suspect.

---

[101] *Id.*

[102] *Terry*, 392 U.S. at 21 (quoting Camara v. Municipal Court, 387 U.S. 523, 536–37 (1967), parentheticals added by *Terry* Court).

[103] SLOBOGIN, *supra* note 95, at 32.

[104] *Katz*, 389 U.S. at 351.

[105] SLOBOGIN, *supra* note 95, at 38.

For critics who tend to find his proportionality principle unworkable, Slobogin explains that the justification for the hierarchy he proposes is virtually identical to the Court's own template: "the probable cause and reasonable suspicion standards are obviously firmly ensconced, the relevance standard is routinely applied in subpoena cases, and the clear and convincing standard is not that far removed from the requirements the Court has imposed in surgery and communications surveillance cases. . . ."[106] Under this approach, vast areas of intrusive police action that are currently unregulated, including physical and transaction surveillance, would no longer be outside the purview of the Fourth Amendment. Slobogin asserts that the proportionality and exigency principles in his book would provide a comprehensive framework, by regulating all government investigative efforts, while remaining flexible enough to allow law enforcement the ability to be proactive in solving crimes.

V. CONCLUSION

As communications technology advances, it becomes easier to collect information on the growing number of consumers subscribing to GPS services that require constant interaction with towers or satellites. Along with this powerful technology comes a high potential for abuse. In lieu of clear legislation on the issue, the battle between the DOJ and the EFF continues, with district courts left divided over what burden law enforcement must meet prior to accessing real-time tracking data– some favoring the DOJ position and law enforcement's need for information and others following the EFF position and protecting the individual's right to privacy. Until higher courts address the issue of what proof is required before carriers must disclose real-time tracking information to law enforcement, any conclusions to be drawn are strictly regional. Noting the lack of jurisdictional consensus, recent decisions are requesting clear legal standards controlling when the government can collect location information from cell phone companies.[107]

---

[106] *Id.* at 46.

[107] *See* In re App. of the U.S. for an Order Auth. the Use of a Pen Register, 384 F. Supp. 2d 562, 566 (E.D.N.Y. 2005) ("If the government intends to continue seeking authority to obtain cell site location information . . . I urge it to seek appropriate review of this order so that magistrate judges will have more authoritative guidance in determining whether controlling law permits such relief. . . . "); *see also* In re Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005) (expressing "full expectation and hope that the government will seek appropriate review by higher courts so

The privacy violations arising from governmental abuse of GPS data from cellular phones and vehicle tracking systems are vast, thus legislative intervention is imperative. Without legislation specifying the burden, law enforcement must produce before invading individual privacy with GPS technology, courts are free to allow intrusion into formally protected zones of privacy without requiring a high burden of probable cause. Undoubtedly, GPS provides many benefits to its users, but it remains to be seen whether the benefits of such technology will be overshadowed by the potential for government abuse of the information and the subsequent invasions of privacy.

---

that authoritative guidance will be given the magistrate judges who are called upon to rule on these applications on a daily basis.").