2012

GPS Tracking and the Fourth Amendment: The New Frontier in Counterterrorism Efforts

German Rozencranc
Seton Hall Law

GPS Tracking and the Fourth Amendment: The New Frontier in Counterterrorism Efforts

German Rozencranc

I. Introduction

The United States Supreme Court recently granted certiorari and heard oral arguments concerning the warrantless use of GPS devices for suspect-tracking purposes.[1] The Court's ultimate decision will help resolve an existing circuit split as to the legality of such a law enforcement practice. [2] In making this decision, the Court is certain to weigh the framework of the Fourth Amendment and utilize the reasonableness assessment that dominated search and seizure jurisprudence. In particular, the Court will deal with the parameters established in *United States v. Knotts,*[3] which held that warrantless beeper monitoring is permissible, and *United States v. Kyllo,*[4] which limited law enforcement ability to use infra-device to scan a home for narcotic-growing machinery.

It is the position of this paper that warrantless GPS tracking can be rationalized through the "special needs" exception to the Fourth Amendment warrant requirement. Using the *United States v. Berger* two-step assessment, it is clear that in the wake of September 11, 2001, GPS tracking is necessary for national security and counterterrorism efforts. Moreover, the practice is made permissible through an existing statutory scheme, the Uniting and Strengthening

---

[1] United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *cert. granted* United States v. Jones, 131 S. Ct. 3064 (2011).
[2] See *infra* Section II, part 1.
[3] United States v. Knotts, 460 U.S. 276 (1983).
[4] Kyllo v. United States, 533 U.S. 27 (2001).

America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act. [5] Finally, the capability to use GPS tracking data for suspect profile creation has become an indispensible tool for achieving a compelling government interest, the halting of terroristic threats.

This paper begins by briefly discussing the framework behind the creation of the Fourth Amendment, the rise of the *United States v. Katz*'s general expectation test, and the degree of privacy that vehicles have obtained in Fourth Amendment case law. Using this background, the second part of this paper deconstructs the present circuit split utilizing the *Berger* framework. It rationalizes the use of GPS tracking through the "special needs" exception by showing that the terrorist attacks of September 11, 2001, resulted in a compelling governmental interest of ensuring domestic safety. Moreover, I argue that there is an existing statutory scheme for permitting such practices and that warrantless GPS tracking is necessary to further this regulatory scheme. I conclude by discussing the implication of this decision and concerns that warrantless GPS tracking could translate to abuse and eventually lead to cell phone tracking.

II. The Fourth Amendment and the Rise of the General Expectation Test

The Fourth Amendment was the product of early American inhabitants' dual concern over the privacy of their home and papers against the government and fear of unbridled official power and discretion.[6] The Fourth Amendment embodied the Founder's trepidation of general warrants and writs of assistance as indicated by several pre-constitutional search and seizure

[5] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT") Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered titles of U.S.C.).

[6] Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325 (2002).

cases including: *Wilkes v. Wood*[7], *Entick v. Carrington*[8], and the Writs of Assistance Case.[9] Embodying the framers' concerns over unbridled executive authority, the Fourth Amendment became a staple against intrusion.[10]

Based on the need to protect the "people" from unrestrained governmental intrusion, the Fourth Amendment stands as a compromise; allowing a right to security for citizens and a restrained governmental authority to maintain order. The text of the amendment reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to go be seized." [11] The first clause has been interpreted to provide a comprehensive right of citizens to be secure against unreasonable searches and seizures.[12] The second clause refers to the issuance of warrants and has a specific purpose of regulating warrant authority.[13] Its effects have been to ban the use of general warrants and mandate a distinct level of specificity prior to the issuance of any such warrant.[14]

---

[7] 19 Howell's State Trials 1153 (K.B. 1763). This case involved Wilkes, a critic of King George II who was awarded damages by Lord Camden after the King's henchmen broke into Wilkes' home and rummaged through is personal papers.

[8] 19 Howell's State Trials 1029 (K.B. 1765). This case involved the King's messengers, who broke into the home of John Entick, a writer, seized his personal papers and eventually arrested him. The messengers were acting pursuant to a search authorization of the Secretary of State for the Northern Department. The Court held that the search was neither authorized by statute or precedent and, therefore, was impressible. Led to the principle that the Government may not act unless explicitly authorized by the law. Cuddihy, William; Hardy, B. Carmon (1980). "A Man's House Was Not His Castle: Origins of the Fourth Amendment to the United States Constitution". *William and Mary Quarterly* (Omohundro Institute of Early American History and Culture) 37 (3): 372–400.

[9] See M.H. Smith, The Writs of Assistance Case (1978). This case involved a challenge of 63 merchants to British customs officers' authority to conduct general searches smuggled goods without particular authorization.

[10] Ku, *supra 1*, at 1332-133.

[11] U.S. Const. amend. IV.

[12] Thomas Y. Davies, *Recovering The Original Fourth Amendment*, 98 MICH. L. REV. 547, 557–58 (1999).

[13] Id.

[14] Id.

The United States Supreme Court has infused Fourth Amendment jurisprudence with an emphasis on reasonableness.[15] Searching for a tool by which to analyze Fourth Amendment challenges, the Supreme Court developed the "reasonable expectation" test in *Katz v. United States.*[16] In particular, the Court held that Fourth Amendment protection applies only in settings where there is a subjective expectation of privacy that is exhibited and where the expectation of privacy is objectively reasonable to society.[17] One's home is rightfully within a zone of protection as a homeowner expects a degree of privacy from intrusion and, correspondingly, society embraces this expectation as being reasonable. Pursuant to this decision, Fourth Amendment protection has been gauged based on an individual's expectation of privacy and, subsequently, the degree of reasonableness to which society embraces said expectation. This analysis led to the rise of different zones of privacy with the most protection given to a person's body[18], followed by a person's home[19] and its curtilage[20], and a severely diminished expectation within the public sphere.[21] While some challenge the use of a reasonableness assessment,[22] it is undisputed that, presently, any future decision concerning the Fourth Amendment must endure

---

[15] *See* California v. Acevedo, 500 U.S. 565, 583 (1991) (Scalia, J., concurring) (asserting "the first principle that the 'reasonableness' requirement of the Fourth Amendment affords the protection that the common law afforded"); Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 652 (1995) ("As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a government search is 'reasonableness.'"); Whren v. United States, 517 U.S. 806, 817 (1996) ("It is of course true that in principle every Fourth Amendment case, since it turns upon a 'reasonableness' determination, involves a balancing of all relevant factors.")

[16] Katz v. United States, 389 U.S. 276 (1960).

[17] Id. at 361.

[18] United States v. Flores-Montano, 541 U.S. 149, 152–53 (2004)(finding that a search of a person's body deserves a higher degree of scrutiny and level of suspicion on the part of the searching parties).

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

[20] United States v. Dunn, 480 U.S. 294 (1987).

[21] Oliver v. United States, 466 U.S. 170 (1984) (discussing that there is no legitimate expectation of privacy in the public sphere).

[22] Lee, Cynthia, Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness *Analysis*, GWU Law School Public Law Research Paper No. 576; GWU Legal Studies Research Paper No. 576. (concern that Implicit bias may also lead courts to exercise their discretion to decide whether a search is reasonable in ways that favor law enforcement and disfavor Blacks and Latinos who make up the bulk of individuals arrested, tried, and convicted of crimes in the United States).

reasonableness scrutiny: gauging a subjective expectation of privacy with society's willingness to embrace it.

i. Vehicles and the Law: Understanding the Present Split.

The motor vehicle has been afforded only limited Fourth Amendment protection due to diminished expectation of privacy one has in their automobile.[23] Since *Chadwick v. United States*, the United States Supreme Court has consistently held that car owners, passengers, and operators are entitled to a reduced degree of expectation of privacy in their motor vehicles.[24] The Court explicitly notes that "[O]ne has a lesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one's residence or as the repository of personal effects…. It travels public thoroughfares where both its occupants and its contents are in plain view."[25] The Court rationalized that automobiles are operated on the open highway and are consistently subject to plain view intrusion.[26] Moreover, cars must be licensed which encompasses a highly regulated operations including a myriad of rules.[27] Finally, automobiles are required to periodically undergo official inspections and are even taken into police custody in the interest of public safety.[28] Combined, these factors amount to a reduced expectation of privacy that permits leeway in automobile searches and seizures.

---

[23] Chadwick, *infra* 19.
[24] United States v. Chadwick, 433 U.S. 1, 12–13 (1977)(reaffirming the Carroll Doctrine's automobile expectations with the added rationale that in addition to a car's mobility, a reduced expectation of privacy permits the search of a car upon the finding of probable cause that the car contained contraband and that it not practicable to obtain a warrant).
[25] Id. at 12 (citing Cardwell v. Lewis, 417 U.S. 583, 590 (1974)).
[26] Id.
[27] Id.
[28] Id.

In a seminal case concerning automotive tracking, the Court upheld the use of a beeper device for tracking purposes in a drug related investigation.[29] The beeper apparatus emitted signals that could be picked up by a radio receiver inside a container of Chloroform.[30] In *United States v. Knotts*, officers followed Knotts after his purchase of Chloroform, using visual surveillance and radio signal tracking, eventually leading to the finding of a drug lab.[31] Confronted with this advance in technology coupled with the reduced expectation of privacy in cars, the Court held that monitoring beeper signals did not violate any legitimate expectation of privacy.[32] The Court explained that tracking a beeper is akin to the following of an automobile on public streets and that there is no expectation of privacy of having a car observed arriving on one's premises after leaving a public highway.[33] Relying on *Knotts,* lower courts have condoned law enforcement officers' use of tracking devices without prior warrant authorization. The decision, however, was not without flaws as indicated by Justice Brennan's concurrence expressing concern that had the defendant challenged not merely certain aspect of the monitoring of the beeper but also the original installation, the Court would have had a much more difficult time addressing the matter.[34]

The Court expanded on the degree to which technology may be utilized without a warrant. Nearly 20 years following *Knotts*, the Court decided *Kyllo v. United States* which involved the use of a heat seeking device officers utilized to scan a home for heat lamps commonly used to grow marijuana.[3536] The Court held there is a minimal expectation of privacy

---

[29] United States v. Knotts, 460 U.S. 276 (1983).
[30] Id.
[31] Id. at 279.
[32] Id. at 282.
[33] Id.
[34] Id. at 286–87 (Brennan, J., concurring).
[35] Kyllo v. United States, 533 U.S. 27 (2001).
[36] Id. at 29.

that protects against the use of sense enhancing technology to obtain information regarding the anterior of a home that "could not otherwise be obtained without physical intrusion into a constitutionally protected area."[37] While visual observation is normally not a search at all, here, the technological advent permits a breach of the home and, therefore, a search took place and a warrant is required.[38] The Court based its decision on two major premises: first, the home is entitled to special protection and, second, the technology in question was not in general public use.[39]

The Circuit courts were left to reconcile these two decisions in the context of Global Position System (Hereinafter "GPS") surveillance. GPS tracking involves the use of a device that is attached to the exterior of a car which omits a signal and is subject to continuous monitoring and data collection.[40] A GPS has three main components including a network of satellites that transmits ranging signals, a control segment maintaining GPS through a system of ground- monitor stations and satellite upload facilities, and user-receivers that process signals of at least four of these satellites.[41] The GPS device uses the signaled information to mathematically determine the receiver's location, velocity, and time in a process known as trilateration.[42]

While GPS tracking was originally developed in the early 1970s by the United States Department of Defense, the technology has since been utilized on a large mass scale.[43] With wide usage, the number of GPS satellites has additionally increased from the original twenty-

---

[37] Id. at 32.
[38] Id.
[39] Id.
[40] Elliott Kaplan and Christopher Hegarty, Understanding GPS: Principles and Applications, (2nd ed. 2006).
[41] Adam Koppel, *Warranting a Warrant: Fourth Amendment Concerns Raised by Law Enforcement's Warrantless Use of GPS and Cellular Phone Tracking*, 64 U. MIAMI L. REV.1061, 1063–64 (2010).
[42] Id.
[43] Ahmed El-Rabbany, Introduction to GPS: The Global Positioning System 1 (1st ed. 2002).

four in 1994 to the present thirty satellite system, thereby permitting greater operability and accuracy.[44] Currently, a basic receiver can accurately determine its position within a few meters.[45] A more advanced GPS system is able to utilize differential data to improve its positing accuracy to within centimeters.[46] Moreover, weather conditions do not affects GPS monitoring, thereby truly permitting continuous positioning and timing information.[47] Technological advances in GPS machinery made its data output all the more accurate and continuous, leading to great advances within the public and reliance by police officers for surveillance purposes.

In its signal emitting capacity, GPS tracking is akin to the beeper tracking that was found permissible in *Knotts.*[48] GPS tracking generally take place outside the scope of the home and is a technology that is presently in widespread public use. These aforementioned factors distinguish GPS tracking from the infra-thermal context that *Kyllo* confronted, yet, the Supreme Court has not tackled the decision directly.[49] GPS tracking, however, presents an additional privacy intrusion given its record-keeping function. With continuous data output, officers may deduct a pattern of behavior and insight into a person's private movements that is not available with either visual or beeper tracking.[50] This led to much confusion amongst the Circuits leaving the matter highly disputed and subject to different interpretations.

Each circuit has handled this issue somewhat differently, yet two schools of thought have eventually emerged. The majority of the circuit courts side with a permissive interpretation of

---

[44] Id., *supra* 25.
[45] Id.
[46] Id.
[47] Id.
[48] Katz, *supra* 16.
[49] Oliver, *Supra* 21.
[50] Berry, *Supra 66*.

Knotts[51] allowing police officers to track potential suspects without probable cause or the procurement of warrants.[52] The minority is represented by the D.C. circuit which requires a showing of probable cause and warrant authorization prior to GPS tracking.[53] Courts, however, have differed on what showing is necessary prior to police officer's use of tracking devices. The 1st Circuit, prior to *Knotts* indicated a hesitation to permit tracking in the context of beepers installed without a warrant.[54] The court stated that officers should have some evidentiary support prior to tracking.[55] In that case, the officers had probable cause to utilize the tracking machinery, yet, the court added that a lesser standard would have sufficed.[56] While eventually the 1st Circuit defaults to *Knotts*, it did not explicitly abandon its requirement that office engaging in surveillance have some basis in fact prior to such monitoring.[57] This default approach has been embraced by the 2nd[58] and 3rd[59] circuits as well, all of which indicate that groundless tracking is not permitted and some evidentiary basis is required.

The 5th and 8th Circuits have required that officers have reasonable suspicion prior to monitoring suspects with GPS tracking. This intermediary standard requires that officers have some reasonable suspicion that criminal activity is taking place and invasive surveillance is,

---

[51] Kyllo, *Supra* 19.
[52] *See generally* United States v. Sparks, 755 F. Supp. 2d 384 (2010); Morton v. Nassau County Police Dep't, 2007 U.S. Dist. LEXIS 87558 (E.D.N.Y. Nov. 27, 2007); United States v. Berry, 300 F. Supp. 2d 366 (D.M.D. 2004); United States v. Hernandez, 647 F.3d 216 (5th Cir. 2011); United States v. Walker, 771 F.Supp. 2d 803 (2011); United States v. Garcia, 474 F.3d 994 (7th Cir. 2007); United States v. Marquez, 605 F.3d 604 (8th Cir. 2010); United States v. McIvar, 186 F.3d 1119 (9th Cir. 1999); United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010).
[53] United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).
[54] United States v. Moore, 562 F.2d 106 (1st Cir. 1977).
[55] Id.
[56] Id. at 111.
[57] United States v. Sparks, 755 F.Supp.2d 384 (2010).
[58] Morton v. Nassau County Police Dep't, 2007 U.S. Dist. LEXIS 87558 (E.D.N.Y. Nov. 27, 2007) (holding that following Knotts, there is no reasonable expectation of privacy in one's movements on public ways, and there was no search or seizure by the placement of a GPS to a vehicle based upon previous sighting of residential burglaries).
[59] United States v. Hosbbach, 518 F.Supp. 759 (E.D. Pa. 1980) (holding that prior judicial authorization is unnecessary to a bumper beeper installation).

therefore, necessary. Pre *Knotts*, the 5th Circuit explicitly held that the warrantless attachment of an electric device to the exterior of a suspect's vehicle, based upon reasonable suspicion, was permissible.[60] Similarly, the 8th Circuit indicated that when police have "reasonable suspicion" that a specific vehicle is transporting drugs; a warrant is not required to install "non-invasive" GPS tracking for a "reasonable period of time."[61] While both circuits defaulted to a *Knotts* type analysis,[62] neither court has explicitly abandoned its intermediary standard of investigation. The 6th Circuit was swayed by *Knotts* and the 8th Circuit's decision in *Marquez.* [63] Pre-*Knotts*, The 6th circuit held that a request for beeper tracking was unreasonable when it did not explicitly specify a time limitation.[64] The court later sided with the 8th Circuit in holding that attaching a tracking device based on police's reasonable suspicion that a vehicle is transporting drugs is permissible and is not a search.[65] The 4th Circuit has indicated some concern about applying a Knotts-beeper type analysis to the GPS context.[66] The Court detailed the difference between a beeper that merely helps the police stay in contact with the vehicle that they are actively monitoring as opposed to a GPS system that wholly substitutes police surveillance.[67] Moreover, the recording of GPS information could amount to severe intrusion and the court indicated that Supreme Court could opt for a warrant requirement based on the degree of intrusion.[68]

---

[60] United States v. Michael, 645 F.2d 252 (5th Cir. 1981).
[61] United States v. Marquez, 605 F.3d 604, 610 (8th Cir. 2010).
[62] Id.; United States v. Hernandez, 647 F.3d 216 (5th Cir. 2011) (holding that GPS tracking tagged to the undercarriage of the defendant's brother vehicle was permissible because public streets scan never fall within a home's curtilage and defendant's expectation of privacy is substantially reduced in a vehicle parked in plain view in a public place).
[63] Marquez, *supra* 49.
[64] United States v. Bailey, 628 F.2d 938, 945 (6th Cir. 1980).
[65] United States v. Walker, 771 F.Supp.2d 803 (2011).
[66] United States v. Berry, 300 F.Supp.2d 366 (2004).
[67] Id.
[68] Id.

The 7th and 9th[69] circuits have both held hat GPS tracking is not a search and, therefore, no warrant is necessary. The 7th Circuit explicitly held that there is no search or seizure under the 4th amendment when police attaches a GPS to a vehicle that: 1) does not draw power from the car's engine or battery; 2) does not take up room occupied by passengers or packages; or 3) does not alter the vehicle's appearance.[70] The court there analogized GPS tracking to the use of surveillance cameras and satellites images, neither of which is considered a search in the Fourth Amendment context.[71] The 9th Circuit emphasized the diminished expectation one has in the undercarriage of a vehicle, where GPS tracking devices are traditionally placed, and ultimately concluded that any such installation does not amount to a search.[72]

Conversely, the D. C. Circuit has recently decided *United States v. Maynard*, wherein it held that the continuous GPS monitoring of a suspect for a period of a month was impermissible.[73] Recognizing that prolonged monitoring yields a highly detailed profile of where a person travels, their association, including political, religious, and personal relationships, the court decided that such tracking amounted to a search.[74] The court emphasized that an ordinary person has a reasonable expectation of privacy in their movements, especially within the course of a month.[75] The Court eventually held that *Knotts* did not govern cases such as these and that police officers offended defendant's reasonable expectation of privacy by tracking his movement continuously.[76] *Maynard* contradicts the argument that GPS tracking is akin to a

---

[69] Sparks *Infra* 57; Hosbach, *infra* 59.
[70] United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007).
[71] Id.
[72] United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010); United States v. McIvar, 186 F.3d 1119 (9th Cir. 1999).
[73] United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).
[74] Id. at 562.
[75] Id. at 559.
[76] Id. at 549, 564.

visual surveillance because of the accuracy and degree to which the information is obtained.[77] GPS tracking presents an additional, more invasive facet, in its information capacity, eventually amounting to a movement profile. In the *Maynard* case, this movement profile served as the primary basis for finding that the defendant was involved in a drug dealing conspiracy.[78] The United State Supreme Court has recently granted certification to hear the case and conclusively resolve this dispute.[79] The "special needs" exception to the warrant requirement could provide the basis for the Court's decision that GPS tracking should be permitted as a warrantless practice.

III. Analysis: Rationalizing GPS Tracking Through The Special needs Exception

The Supreme Court has developed a series of exceptions to the stringent warrant requirements of the Fourth Amendment on the basis of many mitigating circumstances.[80] Among these is the "special need" exception wherein if the government search or seizure is designed to effectuate a special need beyond criminal enforcement, the Fourth Amendment analysis shifts from a probable cause inquiry to a balancing of interests.[81] With a lesser standard than probable cause, courts weigh the need for the search pursuant to the governmental interest and existing statutory scheme versus the degree of invasion into a person's right to privacy.[82] Largely favoring a reasonable suspicion standard, courts have gone so far as to permit area

---

[77] Id.
[78] Id.
[79] United States v. Jones, 131 S. Ct. 3064 (2011)[oral argument Nov. 8].
[80] *See generally* The Hot Pursuit Doctrine: Warden v. Hayden, 387 U.S. 294 (1967); Consent: Schneckloth v. Bustamonte, 412 U.S. 218 (1973); Plain View Doctrine- Arizona v. Hicks, 480 U.S. 321 (1987); Motor Vehicle Exception: Carroll v. United States, 267 U.S. 132 (1925); Arizona v. Gant, 556 U.S. 332 (2009). *See also* Mascolo, Edward, Emergency Doctrine Exception to the Warrant Requirement under the Fourth Amendment, 22 BUFF. L. REV. 419 (1972-1973).
[81] Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989); Skinner v. Ry. Labor Executives' Ass'n., 489 U.S. 602, 624 (1989) (holding that an exception applies when a search serves "special government needs" beyond the normal needs of law enforcement; in which case, the search may be reasonable despite the absence of a warrant, probable cause, or even individualized suspicion).
[82] Id.

warrants, safety inspections, [83] and administrative searches of commercial[84] and non-commercial structures. More recently, the Supreme Court expanded warrantless searches, based on reasonable suspicion, in a school setting.[85] The Court upheld the search of a student's purse for cigarettes by reasoning that the search effectuated the state's need to assure a safe and healthy learning environment.[86] Reasonable suspicion has since been upheld as a sufficient standard for protecting citizens' diminished expectation of privacy in schools[87], employment[88], and governmental posts.[89] This expansion indicates a judicial willingness to embrace alternatives to the probable cause standard and an inclination to allow the government to effectuate social policies with invasive means. Such rationalization could permit sufficient justification for GPS tracking in the wake of 9/11 and increased compromising of Fourth Amendment protection on national safety grounds. We, therefore, proceed to examine the reasonableness of GPS tracking through a two step analysis as enunciated the by the Supreme Court in *New York v. Burger.* [90] There, the Supreme Court held that searches pursuant to the "special need" exception must be the product of a substantial governmental interest that informs the regulatory scheme that permits warrantless searches.[91] In this step, the analysis turns on finding a compelling governmental interest and an existing statutory scheme. Secondly, the warrantless inspection must be necessary to further the regulatory scheme and provide for a constitutionally adequate substitute

---

[83] Camera v. Municipal Court, 387 U.S. 523 (1967).
[84] New York v. Burger, 482 U.S. 691 (1987).
[85] New Jersey v. T.L.O, 469 U.S. 325 (1985).
[86] Id.
[87] Id.
[88] Skinner v. Ry. Labor Executives' Ass'n., 489 U.S. 602, 624 (1989). See also City of Ontario v. Quon, 130 S.Ct. 2619 (2010) (holding that where an employee has a legitimate privacy expectation, an employer's intrusion on that expectation ''for non-investigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstance).
[89] Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989.
[90] New York v. Burger, 482 U.S. 691 (1987). The Court in Burger actually divided the reasonableness analysis to a 3-prong inquiry. Here, we coupled the second and third prongs for brevity purposes and similarity in arguments for sufficing them both in this context.
[91] Id. at 702.

for a warrant.[92] GPS tracking fulfills both prongs given the nature of present day national security and sufficient statutory safeguards at tailoring its use.

i. September 11's Impact on Fourth Amendment Landscape and the Creation of a Compelling Governmental Interest

Prior to the September 11 attack, the Supreme Court has consistently upheld the government's special need to protect its citizens from outside threats. As such, suspicionless safety searches in airports, subways, and public buildings have been unfailingly upheld in nearly every court.[93] This was always the case in the context of national border searches wherein courts have upheld the government's need to regulate and protect the entry points.[94] Derived from the government's sovereign right to stop and examine persons and property crossing into the country, border searches allow officials a means to inspect incoming individuals and their belongings without having to obtain a warrant.[95] This exception has been expanded to include searches of areas that the government and reviewing courts found to be the functional equivalent of an international border.[96] This expansion allows officials to conduct "border searches" even in situations where it is not feasible to conduct the search at the actual point of entry. [9798]

---

[92] Id.
[93] *See* United States v. Davis, 482 F.2d 893, 908 (1973) (holding that airport screenings are considered to be administrative searches because they are conducted as part of a general regulatory scheme, where the essential administrative purpose is to prevent the carrying of weapons or explosives aboard aircraft.*)*; Comm. On Commercial Aviation Sec. Et Al., Airline Passenger Security Screening: New Technologies And Implementation Issues 1, 6 (1996).
[94] Kim, Yule, Protecting the U.S. Perimeter: Border Searches Under the Fourth Amendment, CRS Report for Congress (2009).
[95] Id. at 1.
[96] Id.
[97] Id.

Confronted with flat geographical designations of border-types areas has resulted in much confusion about the type of stop officers are conducting when searching parties within those areas.[99]

In a juncture between border searches and vehicles, the Supreme Court found that the dignity and privacy interests that require reasonable suspicion for highly intrusive searches of a person do not apply to vehicles being examined at the border. [100][101] In *Flores-Montano,* custom officials disassembled the gas tank of a vehicle crossing the border only to find 37 kilograms of marijuana.[102] The Court explained that in light of the need to stem the flow of drugs, the government is entitled certain liberties necessary to effectuate its main goal of protecting territorial integrity and its people's safety.[103] In this interpretive vein, lower courts have found that drilling a hole into personal property such a container or a vehicle to explore its interior made the search non-routine but yet still may be permissible given lenient standards. [104] In *United States v. Arnold*, the 9th Circuit has even permitted the search of laptops in the course of a routine border search. [105] Finding that the Supreme Court has only explicitly limited border searches to "intrusive searches of *the person"* and searches resulting in "exceptional damage to

---

[98] United States v. Ramsey, 431 U.S. 606 (1977) (holding that the search of international mail is okay as part of an investigation of a heroine by mail enterprise).
[99] See generally Almedia-Sanchez v. United States, 413 U.S. 266 (1973) (confronting legislation that permitted border searches 100 nautical miles away from a border).
[100] Yule, *supra* 75, at 15.
[101] United States v. Flores-Montano, 541 U.S. 149, 152 (2004).
[102] Id. at 150.
[103] Id. at 153.
[104] Kim, *supra 87;* United States v. Robles, 45 F.3d 1, 5 (1st Cir. 1995) (drilling a hole into a metal cylinder transported to an airport on an international flight was a non-routine search); United States v. Rivas, 157 F.3d 364, 367 (5th Cir. 1998) (drilling a hole into a tractor tailor's frame was a non-routine search); United States v. Carreon, 872 F.2d 1436, 1440–41 (10th Cir. 1989) (implicitly requiring that drilling a hole into a camper wall in order to effect a search of its interior required reasonable suspicion to be justified).
[105] United States v. Arnold, 523 F.3d 941, 946 (9th Cir. 2008)

property[,]" the court concluded that laptop searches, like car searches, do not trigger a higher standard beyond reasonable suspicion.[106]

The attack of September 11, 2001, has molded a new phase in American geo-political and legal spheres. Historians, politicians, and legal scholars have uniformly pronounced that September 11 marks a transition in American history with significant consequences in nearly every level of government.[107] In the context of the Fourth Amendment, suspicionless searches at airports and other public places have become more intrusive with advances in technology and judicial leeway permitting for more intrusion.[108] In fact, lower courts have uniformly upheld more intrusive searches as falling within the scope of the "special need" exception.[109] A striking example of this expansion has been the 2nd Circuit's decision upholding a New York City program that called for daily inspection checkpoints at selected subway stations.[110] The Court held that prevention of terrorism is a "special need" that is both immediate and substantial given the threat of terrorism.[111] Moreover, searches were minimally intrusive, lasting only a few seconds and people are able to decline and proceed to find alternative means of transportation.[112] The Court has even gone so far as to indicate that the program's level of effectiveness is not subject to judicial review but rather simply its purpose.[113] This implies that an intrusive program

---

[106] Id. at 946 (citation omitted)(emphasis added).
[107] Mary L. Dudziak, *Introduction* to September 11 In History: A watershed Moment 1, 2, 8 (Mary L. Dudziak ed., 2003); Philip B. Heymann, Terrorism, Freedom, And Security: Winning Without War (2003); Steven G. Brandl, *Back to the Future: The Implications of September 11, 2001 on Law Enforcement Practice and Policy*, 1 OHIO ST. J. OF CRIM L., 133 (2003) ; David Lyon, Surveillance after September 11 (2003).
After September 11, and the Future of North American Integration, 91 MINN. L. REV. 101 (2007).
[108] Marc Rotenberg, *Modern Studies In Privacy Law: Foreword: Privacy And Secrecy After September 11*, 86 MINN. L. REV. 1115 (2002).
[109] United States v. Marquez, 2005 U.S. App. LEXIS 14442 (9th Cir. 2005) (holding that additional security examination was constitutionally reasonable where the passenger was randomly selected for more intrusive screening upon or before entering the Transportation Security Administration security checkpoint.)
[110] MacWade v. Kelly, 460 F.3d 260 (2d Cir. 2006).
[111] Id. at 271.
[112] Id. at 265.
[113] Id. at 271.

can be found wholly unworkable and yet be upheld in the courts based on the special need exception. This heightened discretionary standard is akin to judicial leeway in extreme historical cases, such as the State of Emergency exception, and by extension could apply to GPS tracking.[114]

Turning to the first prong of *Berger*, in the wake of September 9/11, grave concern over national security could justify the need to use GPS tracking as a key police instrument. National threats in the form of terrorism have gained their heightened risk standing because of the use of highly technological, covert, and unconventional warfare methodology.[115] National security experts estimate that terrorist factions could very likely reside within the United States leaving police officers with the responsibility to discover these groups and neutralize them.[116] A more permissive approach to police handling of terrorism threats should, therefore, be permitted.

Case law has embraced the dual role of police officers serving as law enforcement officials and counterterrorism units. The Supreme Court in *Burger* held that the administrative nature of inspections is not negated simply because the inspectors were law enforcement officials.[117] In fact, police officer's existing security based infrastructure helps to make

---

[114] *See generally* Kim Lane Scheppele, Law in a Time of Emergency (2004). *Scholarship at Penn Law*. Paper 55. Some of the major exceptions—Lincoln's suspension of habeas corpus upon delegation of this power by Congress, the Palmer Raids, the various attempts by President Roosevelt to circumvent judicial disapproval of the economic emergency measures during the Depression, the initiation of martial law in Hawaii during the Second World War, and the detention of Japanese-Americans during that war—are generally portrayed as being unusual and temporary moments in American history, at least in constitutional retrospect. But not all have been legally repudiated. *See, e.g.*, Mark Tushnet, *Defending* Korematsu*?: Reflections on Civil Liberties in Wartime*, 2003 WIS. L. REV. 273 (examining the claim that the U.S. government has often viewed its abrogation of individual rights during security crises as unnecessary in retrospect).

[115] *See generally* David Tucker, *What's New About the New Terrorism and How Dangerous Is it?,* 13 Terrorism and Political Violence 1 (2001) (finding that new terrorism is a more networked, ad hoc, lethal and dangerous with increased likelihood that a chemical, biological, radiological, or nuclear weapons might be used).

[116] Martin S. Feldstein, *Designing Institutions To Deal With Terrorism In The United States*, National Bureau Of Economic Research, Working Paper 13729 (2008); The National Security Strategy of the United States of America, The President of the United States, 2002.

[117] Burger, *supra* 77, at 717 (noting that "we fail to see any constitutional significance in the fact that police officers, rather than "administrative" agents, are permitted to conduct the § 415-a5 inspection.").

counterterrorism efforts more efficient.[118] Some of the many strengths include: ability to conduct covert intelligence, disruption and dismantling of plots, risk analysis, target hardening, community mobilization, protection of persons and infrastructure, emergency assistance after attacks, order-maintenance during and after attacks, mitigation of damage, and criminal investigation of incidents. [119] State and Federal bodies, in enacting post 9/11 responses, have emphasized the benefits of police force utilization for counterterrorism purposes.[120] This is especially evident by the creation of New York City's Counterterrorism Bureau. [121] Noting that New York City has experienced first-hand the threat of international terrorism, the New York City Police Department Counterterrorism Bureau was formed allowing for a city-wide operation to assist in the prevention of terrorist threats. [122] The NYPD has increased its anti-terrorism division from 17 to 125 detectives and supervisors, and works with FBI agents on terrorism investigation.[123]

The nature and importance of national security coupled with the need to use police officers for counterterrorism purposes amounts to a significant governmental interest that would justify more invasive surveillance methodology. It is undisputed that the Government has a tremendous interest in protecting its people from existing threats and would, therefore, condone use of technological innovation for efficiency purposes. GPS tracking is a crucial adjunct to

---

[118] David H. Bayley and David Weisburd, *The Role of the Police in Counterterrorism*, To Protect and To Serve: Policing in an Age of Terrorism, New York (2009).
[119] Id.
[120] Id. For other benefits of having police officers serve as counter-terrorism agents see the following list: observation and contact during routine patrolling and law-enforcement, analysis of crime patterns indicative of terrorism preparation, forming partnerships with local businesses and communities of interest, using local knowledge to assess the validity of intelligence produced by specialized counterterrorism agencies, contributing local expertise in covert surveillance and penetration, and developing informers through leverage over local criminals.
[121] The City of New York, Counterterrorism Units, *available at* http://www.nyc.gov/html/nypd/html/administration/counterterrorism_units.shtml
[122] Id.
[123] Id.

counterterrorism surveillance efforts, amounting to a substantial governmental interest in promoting its use in a variety of police oriented tasks.

ii. Existing Statutory Scheme and the No Alternative Route

Having established a compelling governmental interest in the use of GPS tracking for police counterterrorism efforts, such use must be pursuant to an established statutory scheme.[124] The Court has repeatedly held that unbridled police discretion would not be permitted and a statutory scheme is, therefore, necessary to regulate police conduct. [125] In an immediate response to the 9/11 attack, Congress enacted the Uniting an Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (hereinafter "Patriot Act").[126] The Act codified a federal case law trend that broadly interpreted the Fourth Amendment search and seizure provisions.[127] The Patriot Act, accordingly, moved further away from the probable cause standard. The Patriot Act reduces restrictions on law enforcement agencies seeking to search telephone, email communicational, financial and medical records, and generally investigate suspects.[128] In particular, Section 213 and 218 have created tremendous amount of uproar in expanding the authority for surveillance under the Foreign Intelligence Surveillance Act and condoning "sneak and peek" authority, allowing agents executing search

---

[124] Burger, *supra* 77, at 702.
[125] Florida v. Wells, 496 U.S. 1 (1990).
[126] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT") Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered titles of U.S.C.).
[127] *See* Charles Doyle, Congressional Research Service Report Rl31200: Terrorism: Section By Section Analysis Of The USA Patriot Act (2001) *available at* ttp://www.cdt.org/security/usapatriot/011210crs.pdf
[128] Susan N. Herman, *The USA PATRIOT Act and the Submajoritarian Fourth Amendment*, 41 HARV. C.R.-C.L. L. REV. 67 (2006).

warrants to delay telling the targets that their property has been searched or seized. [129] Section 218 particularly expanded the government's authority to use FISA warrants to conduct electronic surveillance instead of proceeding under the demanding standard of Title II which cover criminal investigation.[130] These expansions circumvent Fourth Amendment safeguards by legislative means that omit governmental action from judicial review at its inception. While subsequent judicial review is feasible, the Government and judicial interpretation of the Act indicate that this statutory scheme succumbs to governmental deference at the cost of greater protection of Fourth Amendment provisions.

More relevant to the GPS analysis is the Patriot Act's expansion of the definition of terrorism to include domestic terrorism.[131] Specifically, the Act defines the term "domestic terrorism" to include any activities that involve "acts dangerous to human life *that are a violation of the criminal laws* of the United States or of any state." [132] This wording amounts to a grounds for which law enforcement bodies may utilize GPS tracking for criminal investigation purposes under the guise of terrorism prevention. Regarding the level of suspicion necessary for the police to have before engaging in GPS tracking, the Act simply requires that suspected

---

[129] Id. at 72–3.
[130] Id. at 92.
[131] Domestic Terrorism Defined- Section 2331 of title 18, United States Code, is amended--
(1) in paragraph (1)(B)(iii), by striking `by assassination or kidnapping' and inserting `by mass destruction, assassination, or kidnapping';
(2) in paragraph (3), by striking `and';
(3) in paragraph (4), by striking the period at the end and inserting `; and'; and
(4) by adding at the end the following:
(5) the term `domestic terrorism' means activities that--
(A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
(B) appear to be intended--
(i) to intimidate or coerce a civilian population;
(ii) to influence the policy of a government by intimidation or coercion; or
` (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
(C) Occur primarily within the territorial jurisdiction of the United States.'-
Patriot Act, P.L. 107-56, Title VII Section 802.
[132] Id. (emphasis added).

activities "appear to be intended- (i) to intimidate or coerce a civilian population; (ii) to influence the police of a government by intimidation or coercion; or (iii) to affect the conduct of a government[.]"[133] The "appear to be intended" standard is much less than the probable cause requirement that is necessary to obtain a warrant and indicates the permissive nature of counterterrorism practices.

Recognizing that terrorism could emerge from within the United States, the Act also includes the "Lone Wolf" provision[134] which allows intelligence investigations of terrorist suspects not connected to a foreign nation or organization. A broad reading of this provision gives nearly unrestricted discretion for police officers to investigate citizens without having to prove that they belong to a foreign terrorist organization.[135] GPS tracking, therefore, is likely permissible within the scope of the Patriot Act, allowing for greater data retention, at minimal cost, of these suspected individuals. The regulatory scheme here is non-discriminatory and invasion is minimal when compared to some of the more draconian allowances the Act permits including the "sneak and peek" scenarios. Police usage of GPS tracking, therefore, would be considered highly regulated endeavor that is pursuant to a statutory scheme that aims to minimize national and domestic threats. The fact that police officers have some discretion as to who they investigate does not undermine the non-discriminatory end of GPS tracking. The Supreme Court has conclusively noted that police discretion is permissible so long as the discretion is exercised according to standard criteria on the basis of something other than suspicion of criminal activity.[136] Here, police investigation would be pursuant to the Patriot Act's

---

[133] Id.
[134] Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004
[135] Doyle, *supra* 110.
[136] Colorado v. Bertine, 479 U.S. 367, 376 (1987).

definition of domestic terrorism which permits law enforcement permissible discretion to classify parties as such without a reviewing intermediary body.

In general, "special needs" based exceptions are subject to the limitation that once a regulation is primarily used for crime prevention or evidence gathering instead of some other compelling governmental interest, such exception becomes inapplicable and general Fourth Amendment standards apply. [137] Regulations with a dual purpose of promoting a governmental interest and assisting in crime prevention, however, have repeatedly been found permissible so long as the governmental interest is the primary reason for the practice. In fact, a secondary purpose of crime prevention has generally been permitted in the context of "special need" exceptions.[138] In *City of Indianapolis v. Edmond,* the Court explicitly noted that a secondary criminal prevention purpose is permissible so long as the regulation's primary purpose is "non-law enforcement" related.[139] The fact that GPS tracking would serve substantial criminal evidence gathering function would not invalidate it as the primary function is nonetheless attributed to national safety efforts. With a primary non-law enforcement related purpose, the Patriot Act has permitted the Government to no longer differentiate between information gathered for criminal purposes and surveillance for the purpose of gathering foreign

---

[137] Ferguson v. City of Charleston, 532 U.S. 67 (2001) (holding that once the immediate objective of the program was to generate evidence of law enforcement purpose, it can no longer bypass Fourth Amendment Requirements).
[138] *See* City of Indianapolis v. Edmond, 531 U.S. 32 (2000) progeny cases that upheld checkpoints where the articulated primary purpose effectuate a special beyond law enforcement even those there is a secondary purpose. See United States v. Davis, 270 F.3d 977 (D.C. Cir. 2001); United States v. Moreno-Vargas, 315 F.3d 489 (5th Cir. 2002).
[139] City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000).

intelligence.[140] In so permitting, the Patriot Act circumvents previous judicial safeguards that mandated stricter standards for criminal based investigation and enforcement.[141]

Turning to the second prong, warrantless inspection must be necessary to further the regulatory scheme. In enacting the Patriot Act, Congress related the urgency with which national threats must be addressed, therein permitting for a circumvention of the Fourth Amendment regulations. The preamble to the Act alone indicates that the purpose of the legislation involves national safety interests that cannot be sufficed but for the statutory tools the Acts now permits.[142] While the Act does explicitly name some of these warrantless tools including authority to intercept wire, oral, and communication; it additionally allows the enforcing agents leeway in choosing appropriate methodology by which to carry on the purpose of the Act.[143] As such, police may turn to the GPS tracking as a distinctly effective surveillance method.

The use of surveillance, for national security purposes, has been a fundamental tool for a variety of governmental purposes. Three relevant functions of surveillance include "to anticipate a violation…to detect a violation…or to assist in the identification of the person responsible for a violation or in the authentication of an assertion as to the identity of a culprit."[144] Since the inception of GPS technology, advents in commerce and globalization have increasingly led to the proposition that the ability to collect data equates to having power.[145] From a national defensive standpoint, the ability to collect data, in real time, provides invaluable tools for preempting

---

[140] Richard Henry Seamon and William Dylan Gardner, *The Patriot Act And The Wall Between Foreign Intelligence And Law Enforcement*, 28 HARV. J.L. & PUB. POL'Y 319 (2004).
[141] Paul Rosenzweig, *Civil Liberty and the Response to Terrorism*, 42 DUQ. L. REV. 663, 688 (2004) (provisions in Patriot Act "tear down the wall").
[142] Patriot Act, P.L. 107-56, Preamble- "To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes."
[143] Id. Title II, Section 202 and 203.
[144] Holly Tootell, *Auto-ID and Location-Based Services in national security: Social implication,* The Second Workshop on the Social Implication of National Security (2007).
[145] Id. at 210.

various threats. The rise of the Department of Homeland Security as an indispensible governmental agency indicates the degree to which domestic safety plays in present times. National security, accordingly, has been expanded to include "intelligence gathering and warning, border and transportation security; domestic counter terrorism; protection of critical infrastructure; defending against outside attacks; and emergency preparedness and response."[146] With the threat of terrorism looming and the limitedness o state resources, state police actors have turned to technological advents to combat an unknown, sophisticated enemy.[147]

Officers, accordingly, rely on GPS technology to gather invaluable insight as to the present location of tracked suspects.[148] Especially helpful to counterterrorism efforts is the ability to compose a location profile of monitored individuals.[149] Profile formation, using GPS tracking, has proven to accurately model human behavior and provide private insight into people's lives.[150] In addition to successfully monitoring individuals, GPS tracking provides for a greater threat unearthing. Terrorists often work in cells and GPS tracking of one suspected terrorist could easily unearth a network of terrorists with relatively few logistical costs. [151] Requiring officers to obtain individual permission to GPS track would unduly burden law enforcement agents, decelerate terrorism prevention, and work to contradict the intent behind the Act's promulgation. Warrantless GPS tracking, therefore, is necessary to permit for an efficient, minimally invasive system to tracking that helps law enforcement agents quickly preempt terrorist threats.

---

[146] Office of Homeland Security, *National Strategy for Homeland Security* (2002).
[147] Hasinchu Chen, *Intelligence and Security Informatics for International Security* (2006).
[148] El-Rabbany, *Supra 32*.
[149] Id.
[150] Michael, K, McNamee, A, Michael, MG and Tootell, H, *Location-Based Intelligence – Modeling Behavior in Humans using GPS*, in Proceedings of the International Symposium on Technology and Society, New York, 8-11 June 2006.
[151] Valdis E. Krebs, Mapping Networks of Terrorist Cells (2002), *available at:* http://www.sfu.ca/~insna/Connections-Web/Volume24-3/Valdis.Krebs.web.pdf

The prevalence of national security as a governmental interest combined with the existing Patriot Act scheme; undoubtedly suffice the *Berger* test for a "special need" exception. The realities of September 11 and the need to use technology for counterterrorism purposes highlight the fact that while privacy rights are important, we cannot divorce ourselves from present day reality. The statutory leeway provided by the Patriot Act allows state law enforcement a right to choose the most effective tool for combating national threats. GPS tracking affords surveillance intelligence capabilities that optimize threat prevention with optimal resource utilization.

iii. The Implications of GPS Tracking; When Leeway Turns to Abuse

Opponents of GPS tracking have raised two main contentions to warrantless police surveillance practices. Firstly, use of GPS tracking can easily yield abuse. With no supervisory benchmarks, law enforcement agencies may opt to monitor any party, at any time, for an unrestricted period of time. Failure to require warrants could translate to arbitrary and capricious application of GPS tracking. Of special concern is the magnitude of many citizens' vulnerability to the abuse of GPS monitoring given the prevalent use of motor vehicles in our society.[152] From a policy standpoint, excessive government surveillance could exert a chilling "big brother" effect upon society.[153] GPS tracking could, in essence, transition to a general warrant the Framers hoped to combat with the enactment of the Fourth Amendment.[154]

These concerns have prompted the American Bar Association to issue standards for electronic and physical surveillance. Specifically, the standards advise that "at the outset[…] technologically-assisted. . . surveillance should be regulated not only when it diminishes privacy,

---

[152] Osburn v. State, 44 P.3d 523, 527–28 (Nev. 2002)(Rose, J., dissenting).
[153] John S. Gonz, *It's Already Public: Why Federal Officers Should Not Need Warrants To Use Gps Vehicle Tracking Devices*, 95 J. CRIM. L. & CRIMINOLOGY 1325 (2005).
[154] *Supra* 1.

but also when it diminishes 'freedom of speech, association and travel, and the openness of society.'"[155] Despite the legitimacy of these concerns, placing a warrant requirement on police tracking would be excessive. Instead, internal regulation could provide sufficient safeguards without triggering strict constitutional protections.[156]

Secondly, GPS tracking, by extension, could amount to police officers tracking individuals utilizing citizens' own cellular devices. While the United States Supreme Court has not certified this issue on appeal, commentators have expressed concern that permissive warrantless GPS tracking could transition to government access to cellular GPS location data.[157] Presently, there are more than 262 million cellular-phone subscribers in the United States. [158] Cellular phones relay their location to phone towers to have the strongest possible signal and promote inbound calls from being interrupted. [159] This process is called "registration" and occurs every seven seconds automatically, without any user interaction.[160] Cellular towers transmit and store this information for providers' billing purposes. Additionally, many cell phone devices are equipped with GPS chips that permit users to operate their phones as GPS devices. Through triangulation, cell phone towers use cell phone signals to calculate the Time Difference of Arrivals and the Angle of Arrival to proximately locate a cell phone user's location.[161]

---

[155] Id. at 1359 (citing David Heinzmann, Smile, You're On Candid Cop Cam, Chi. Trib., Feb. 25, 2005).
[156] Id.
[157] Derek P. Richmond, *Can You Find Me Now?-Tracking the Limits on Government Access to Cellular GPS Location Data*, Commlaw Conspectus (2007).
[158] Adam Koppel, *Warranting a Warrant: Fourth Amendment Concerns Raised by Law Enforcement's Warrantless Use of GPS and Cellular Phone Tracking*, 64 U. MIAMI L. REV. 1061, 1066 (2010).
[159] Id. at 1067.
[160] *See* Posting of Tom Farley & Mark van der Hoek to Privateline, http://www.privateline.com/mt_cellbasics (Jan. 1, 2006).
[161] Koppel, *supra* 153, at 1067.

Combined, these features are very desirable for law enforcement agencies that can use this information to determine a suspect's approximate location and to track his or her movement.[162]

Electronic surveillance is generally governed by the Electronic Communications Privacy Act of 1968 (hereinafter "ECPA").[163] Pursuant to the ECPA, law enforcement officers may obtain a court order that would require cellular service providers to turn over location tracking information.[164] There is, however, a split among both the state courts and appellate circuit courts as to the legal standard required for obtaining prospective, real time information from third-party cellular providers.[165] The standards depend on what aspect of the ECPA the courts believe is implicated. Specifically, the Act is divided into three titles which courts have deconstructed to four categories of protection. Firstly, Title I of the ECPA, which address the interception of wire, electronic, and oral communication, provides the most protection for cellular communication in forcing the government to meet "super warrant requirements" before the interception of conversation content.[166] Secondly, Title II of the Act addresses the government's burden of obtaining customer records which requires a "showing of specific and articulable facts regarding the government's needs for the information.[167] Thirdly, concerning authority required for use of a tracking device, the government must show probable cause.[168] The final category involves the use of pen registers and "trap and trace" devices, which pursuant to Title III,

---

[162] Id. at 1068.
[163] 18 U.S.C. §§ 2510–2522 (2006).
[164] Koppel, *supra* 153, at 1068.
[165] Compare Diaz, *infra* 170 with In re Applications of United States of America for Historical cell Site Data, *infra* 172.
[166] Id. (citing 18 U.S.C. § 2518 (2006)).
[167] Id. at 1080 (citing § 2703(d)).
[168] Id. at (citing § 3117(a)).

requires the government to simply demonstrate the material is relevant to an ongoing criminal investigation.[169]

Given the breadth of ECPA interpretations, it is not surprising that courts varied on the legal standard necessary for the government to obtain cell-phone data from cellular providers. For example, the California Supreme Court has recently decided that police officers may obtain cell phone texting records without a warrant.[170] The court reasoned that because the cell phone was "immediately associated with defendant's person[,]" officers were entitled to inspect its content, without a warrant, regardless of whether an exigency existed.[171] Conversely, the United States District Court for the Southern District of Texas recently decided that "[w]hen the government requests records from cellular providers, data disclosing the location of the telephone at the time of particular calls may be acquired only by a warrant issued on probable cause."[172]

A decision concerning warrantless GPS monitoring of suspects' vehicles can have significant implications on the capability of officers to obtain cell phone record information. While GPS tracking and cell phone surveillance practices have many aspects in common, there are significant differences that would deter the Court from deciding the *Maynard*[173] decision broadly. In particular, cell phone records implicate a different expectation of privacy from a *Katz*[174] reasonable assessment standpoint. Cell phones generally enter into the home and could provide output information relating to a suspect's presence and location within the home. As

---

[169] Id. at (citing § 3122(b)(2)).
[170] People v. Diaz, 51 Cal. 4th 84 (Cal. 2011).
[171] Id. at 110–11.
[172] In re Applications of United States of America for Historical cell Site Data, H-11-223 (S. Dist. of Tex. 2011).
[173] Maynard, *supra* 68.
[174] Katz, *supra* 11.

such, *Kyllo*[175] is more heavily implicated in this context. Moreover, cell phones have not been the subject of decisions that repeatedly discount the expectation of privacy citizens have in them like vehicles have.[176] In fact, any decisions concerning cell phone data have been interpreted as outdated and superseded by the ECPA enactment.[177] Cell phone data collection and record keeping, while physically entering into the public sphere, cannot be obtained through visual inspection. Instead, steps beyond ordinary police practices must be undertaken for information gathering purposes. The different privacy implications in the cellular context will likely sway the Court to side with a more stringent standard that would require officers to obtain warrants prior to seeking such records. The Supreme Court, however, has repeatedly reinforced its practice of deciding issues narrowly. [178] Given the above differences, the Court will likely limit its decision to the sole issue on the application of a GPS device to a suspect's car and opt to disregard the implications this decision will have on cell phone tracking.

IV. Conclusion

It is undisputed that GPS tracking implicates citizens' expectation of privacy under the Fourth Amendment. *Katz's* reasonableness assessment vindicates the right of people to be secure from governmental intrusion, even in highly susceptible areas such as a motor vehicle on a public highway, by requiring that subjective and objective reasonableness expectations be protected. The right against privacy invasion, however, must be balanced with competing interests that erode the constitutional privilege in favor of greater social welfare. While theoretically constitutional rights are not subject to legislative change, theory must often yields to

---

[175] Kyllo, *supra* 30.
[176] Chadwick, *supra* 19.
[177] *See* United States v. Allen, 1999 CCA LEXIS 116, n. 3 (A.F.C.C.A. 1999) (noting that Smith v. Maryland, 442 U.S. 735 (1979) and other similar decisions have been statutorily overruled.)
[178] Gideon v. Wainwright, 372 U.S. 335 (1963) (noting in dicta that the Supreme Court generally limits its holdings to the particular facts and circumstances of that case).

the pragmatics of reality. In this context, the imposition of GPS surveillance is attenuated by the need to protect the United States from international and domestic threats.

September 11, 2001 accentuated the present risks the United States is facing. Especially alarming has been the revelation that national threats are not solely foreign and parties within the United States are working to cause severe harm to the country and its corresponding citizens. To help mobilize counterterrorism, Congress enacted the Patriot Act to provide wide discretion for law enforcement agencies in their protection efforts. Law enforcements were given the ability to suspend generally accepted constitutional disclosure requirement that follow searches. Additionally, state police agencies were permitted to conduct invasive surveillance efforts on any domestic suspect that the officers reasonably suspected could be a threat to the country. The national interest embodied in the Patriot Act combined with the permissive rights it grants law enforcement officers can, therefore, permit the use of GPS tracking as a routine surveillance practice. The benefits obtained from warrantless GPS tracking, especially, are unmatchable by any other reasonable means. In addition to providing real-time tracking, that would require extraordinary financial means if replicated by police officers, GPS data gathering amounts to an extremely revealing individual profile of a suspect that could unearth a network of other terroristic threats. Accordingly, in relying on *Berger*'s two prong test, there is strong support to classify warrantless GPS tracking as a special needs exception to the warrant requirement.

In granting certiorari on the *Maynard* case, the United States Supreme Court expressed an interest in resolving the present conflict that has developed since the *Knotts* decision. In ultimately deciding the case, the Court will signal its standpoint on technological advents and their implications on citizens' reasonable expectation of privacy. In particular, the Court is

forced to reconcile permissive surveillance tactics with the *Kyllo* decision where the Court pulled back on its permissive view on technological use for police purposes.

Zealous opponents to warrantless GPS tracking emphasize that the decision could create dangerous precedent that would permit further Fourth Amendment erosion. In particular, warrantless GPS tracking could by extension permit law enforcement agencies to mandate third party cellular service providers to handover cell phone user's location and movement history from their own device. Despite these concerns, the Supreme Court has established a policy of deciding decisions very narrowly and likely would not address this matter. Moreover, GPS tracking via a suspect's own cellular device implicates different privacy interests and a separate body of legislative enactments and corresponding case law. As such, the decision will likely be sufficiently tailored to quail most opponents' concerns.

Given the need to protect the United States from terrorist threats, the Fourth Amendment cannot stonewall the use of technological advances. In face of unconventional warfare, the like presented with terrorism, warrantless GPS tracking could be the difference between allowing and preventing another attack on domestic soil. The Fourth Amendment must succumb to a new understanding of what is socially reasonable and concede to an urgent governmental need.