I/S: A Journal of Law and Policy for the Information Society
Winter 2007-2008

Government Surveillance in Context, for E-mails, Location, and Video:

***473** PERSONAL PRIVACY IN THE FACE OF GOVERNMENT USE OF GPS

Kevin Keener [FNa1]

Abstract: GPS units are multiplying around the world and are being used in both vehicles and cellular phones. With the increasing pervasiveness of GPS, law enforcement now has the capability of learning the specific location of a suspect without the suspect's knowledge or consent. This note will examine when law enforcement officials may use GPS to track suspects without a warrant under both federal law and state law. This note will also examine when law enforcement officials may obtain documents from third-party service providers about a suspect's location information.

***474** I. Introduction

On June 26, 1993, the U.S. Air Force launched the 24th NAVSTAR satellite into orbit, completing the network of satellites that make up the Global Positioning System (“GPS”). [FN1] GPS works by measuring the distance from a receiver to four individual satellites to determine a receiver's longitude, latitude, and altitude. [FN2] To “triangulate” a position in this manner, a GPS receiver calculates the distance to each satellite by measuring the time necessary for a radio signal to travel to that satellite. [FN3] Since the development of GPS, receiver units have become relatively widespread and inexpensive. GPS units are now prevalent in automobiles and cellular phones. General Motors offers its GPS service, OnStar, in over fifty models of its 2007 line. [FN4] Verizon Wireless provides GPS-based services that allow subscribers to get directions and search for local points of interest, such as restaurants and ATMs. [FN5] Due to the prevalence of GPS receivers in today's society, the government's power to obtain GPS-based location information has raised privacy concerns.

Cellular phones provide an even more interesting aspect regarding the government's power to obtain personal location information. December 31, 2005, saw the completion of Phase II of Enhanced 911 or “E911.” [FN6] This program, promulgated by the Federal Communications Commission (“FCC”), requires cellular phone service providers to “achieve 95 percent penetration of location-capable handsets among its subscribers.” [FN7] This requirement was ***475** established in response to the growing number of 911 calls originating from cellular phones and the failure of emergency services to access the location of the caller in an emergency situation. [FN8] Pursuant to this rule, service providers have included GPS chips in the cellular phones that they sell. However, obtaining location information through cellular phones is nothing new. Government agents have long been able to access information about the location of a phone's “cell site.” The government can access this information either in real time or for as far back as eighteen months. [FN9]

The current debate on the use of GPS focuses on the level of privacy that consumers of this technology can

expect with the location-related information that is prevalent in this technology. This article will attempt to answer two questions: (1) When may the government use GPS to directly track your location? and (2) When may the government access records of a suspect's location from third-party enterprises that provide GPS services?

There currently is no legislation, either federal or state, restricting the government's use of GPS to track the location of suspects. Absent legislation, only the Fourth Amendment to the Constitution of the United States limits the federal government's use of this technology when it would constitute an unreasonable search or seizure. This paper will consider (1) the limits placed on the federal government's use of this technology under the Constitution of the United States; (2) the limits placed on state governments' use of this technology under respective state constitutions; (3) the alternative method for tracking cellular phones, other than GPS, and relevant statutes concerning the protection of location information from this method; and (4) government access to records of third-party service providers regarding location information. [FN10]

***476** II. The Law Restricting Government Use of GPS

A. Federal Law

There are two ways in which the government may use GPS to identify the location of a suspect: the government may directly attach a GPS unit to a suspect's vehicle or the government may obtain GPS location information (or other technology-based location information) from a current service provider. There currently is no legislation restricting the government's use of GPS.

Absent any legislation, the only protection provided to citizens is the Constitution. The Fourth Amendment provides “the right of the people to be secure in their persons . . . against unreasonable searches and seizures.” [FN11] A search occurs when a government agent infringes on an expectation of privacy that society considers reasonable. [FN12] A seizure occurs when the government interferes with an individual's possesory interest in property. [FN13] Such interference occurs when the government intentionally interferes with the freedom of movement. [FN14]

The Supreme Court of the United States has determined the limits that the Constitution places on government use of tracking technology in two cases: United States v. Knotts [FN15] and United States v. Karo. [FN16] Another Supreme Court case that could have future consequences on government use of tracking technology is Kyllo v. United States. [FN17] Although the issue of the government's use of GPS has not reached the ***477** Supreme Court, many district courts have considered the issue, the most recent of which is United States v. Moran. [FN18]

In United States v. Knotts, Minnesota law enforcement agents installed a beeper in a five-gallon container of chloroform that was suspected of being used to manufacture illicit drugs. [FN19] After the purchase of the chloroform, the agents followed the car carrying the chloroform, maintaining contact through both visual surveillance and monitoring the beeper signals. [FN20] During the tracking of the suspect's vehicle, the suspect began making evasive maneuvers and officers lost both visual contact and the beeper signal. [FN21] Officers eventually regained the signal from the beeper and determined that the signal was stationary and emanating from a cabin. [FN22] Officers used the location of the chloroform derived through the use of the beeper and additional visual surveillance of the cabin to secure a search warrant. [FN23] When executing the warrant, officers discovered a fully operable methamphetamine lab. [FN24] The container of chloroform containing the beeper was

discovered under a barrel outside of the cabin. [FN25]

The Supreme Court held that the warrantless monitoring of the beeper did not violate the defendant's Fourth Amendment right. [FN26] The Court used a two-step analysis originally established by Justice Harlan in Katz v. United States. [FN27] The first step was to determine whether the individual, by his conduct, had exhibited an actual, subjective expectation of privacy. The second step was to determine whether the individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable. [FN28] The Court reasoned that "a ***478** person traveling in an automobile has no reasonable expectation of privacy in his movement from one place to another." [FN29] The fact that agents used a beeper to track the vehicle was immaterial to the Court. The Court reasoned that "a police car following [the suspect] at a distance throughout his journey could have observed him leaving the public highway and arriving at the cabin owned by respondent, with the drum of chloroform still in the car." [FN30] The Court hinted that the defendant's Fourth Amendment right would have been violated had the use of the beeper "reveal[ed] information as to the movement of the drum within the cabin, or in any way that would have not been visible to the naked eye from outside the cabin." [FN31]

Unlike Knotts, the Supreme Court found that government agents violated the Fourth Amendment in United States v. Karo. [FN32] In Karo, DEA agents suspected that a 50-gallon shipment of ether was going to be used to extract cocaine from clothing that had been imported into the United States. [FN33] The agents obtained a court order authorizing the installation and monitoring of a beeper in one of the cans of ether. [FN34] The agents used both physical and electronic surveillance of the shipment while it was being transported along public highways but stopped visual surveillance when the shipment arrived at a house for fear of detection. [FN35] When the vehicles used to deliver the shipment left the residence, agents used the receiver to determine that the beeper was inside the house. [FN36] The agents used the information derived from the use of the beeper to obtain a search warrant for the residence. [FN37]

***479** The Supreme Court held that monitoring the beeper in the private residence, a location not open to visual surveillance, violated the Fourth Amendment right of the defendant who had a justifiable interest in the privacy of the residence. [FN38] The Court held that "private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable." [FN39]

A recent Fourth Amendment case with some bearing on the issue of the use of GPS is Kyllo v. United States. [FN40] In Kyllo, a government agent suspected Kyllo was growing marijuana inside his home. [FN41] The agent used a thermal-imaging device to detect infrared radiation from high-intensity halide lamps inside the residence that were being used to grow marijuana. [FN42] The agent used this information to obtain a search warrant of the residence and found more than one-hundred marijuana plants. [FN43] The Supreme Court determined that the use of the thermal imager constituted a "search" and violated the defendant's Fourth Amendment right. [FN44] The Court declared that when "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." [FN45] This case could have implications in future cases if a court were to determine that GPS has become part of the "general public use" to the extent that government use of it does not constitute an unreasonable search without a warrant.

The most recent federal case involving the challenge of the warrantless use of GPS to track a suspect's vehicle is United States v. ***480** Moran. [FN46] At a trial for narcotics charges, the defendant moved to suppress evidence obtained from a GPS device that was attached to his vehicle without a warrant on the grounds that it

violated his Fourth Amendment rights. [FN47] The court concluded that the use of the GPS device was permissible because "Moran had no expectation of privacy in the whereabouts of his vehicle on a public highway." [FN48] The court noted that because "law enforcement personnel could have conducted a visual surveillance of the vehicle as it traveled on the public highways," there was no search or seizure in the use of the GPS device. [FN49]

B. State Law

A handful of state courts have also considered the need for law enforcement agents to obtain a warrant prior to using GPS to track a suspect. Although law enforcement may use GPS to track a suspect's vehicle without a warrant under the United States Constitution, "the United States Supreme Court has noted that states are free to interpret their own constitutional provisions as providing greater protections than analogous federal provisions." [FN50]

There is currently a split in the states that have considered whether their respective constitutions permit government agents to track suspects with GPS without a warrant. For example, under the California and Nevada Constitutions, law enforcement agents do not need to obtain a warrant to track suspects with GPS. The Louisiana, Oregon, and Washington Constitutions, on the other hand, do require law enforcement agents to obtain warrants. New York courts have considered the issue but the matter remains unresolved.

***481** 1. States Where No Warrant is Required

a. California

The California Sixth District Court of Appeal considered the warrantless use of GPS to track a defendant's vehicle in People v. Zichwic. [FN51] In Zichwic, the defendant had been released from prison and placed on parole subject to the condition that his "residence and any property under [his] control [could] be searched without a warrant by . . . any law enforcement officer." [FN52] Police suspected the defendant's involvement in burglaries and obtained authorization from the defendant's parole officer to conduct electronic surveillance of the defendant. [FN53] Officers placed an electronic monitoring device on the undercarriage of the defendant's truck while it was parked in the defendant's driveway at a multi-unit single story complex. [FN54]

The Zichwic Court determined that the placement of the monitoring device did not violate the defendant's Fourth Amendment right under the California Constitution. [FN55] The Court applied a two-step analysis: first, it looked to the subjective expectation of privacy of the defendant; second, it analyzed the objective expectation of privacy. As to the defendant's subjective expectation of privacy, the Court reasoned that the imposition of the warrantless search provision as a condition of parole diminished the defendant's reasonable expectation of privacy. [FN56] The Court also concluded that there was no objective expectation of privacy:

> There can be no objectively reasonable expectation of privacy in what is regularly exposed to public view. While the undercarriage of a vehicle is not as readily seen as the hood, doors, and other parts of its exterior, the undercarriage is part of the exterior that is ordinarily exposed to public ***482** view. It does not amount to a search to examine the undercarriage, to touch it, or to attach a tracking device, so long as a police officer does so from a place where the officer has a right to be. [FN57]

The Zichwic Court considered whether monitoring the signals from the tracking device constituted a search.

[FN58] The Court, relying on Knotts, concluded that the monitoring of the device did not constitute a search since the monitoring "simply revealed the movements of defendant's truck on city streets." [FN59] Therefore, under the California Constitution, California law enforcement may attach and monitor a GPS device to a vehicle without a warrant.

b. Nevada

The Supreme Court of Nevada considered the warrantless use of a GPS tracker in Osburn v. State. [FN60] In Osburn, as part of a serial rape investigation, police attached an electronic monitoring device to the bumper of the defendant's vehicle in order to track his movements as he traveled on public streets. [FN61] Through visual surveillance and use of the electronic monitoring device, the police observed the defendant committing "voyeuristic activities." [FN62] Police then obtained a search warrant, searched the defendant's vehicle, and found burglary tools and child pornography. [FN63]

In determining whether attaching the electronic device constituted a search or seizure under the Nevada Constitution, the Court applied a two-step analysis: "in order for an unreasonable search or seizure to exist, the complaining individual must have a reasonable expectation of privacy, which requires both a subjective and an objective ***483** expectation of privacy in the place searched or the item seized." [FN64] The Court decided that the defendant exhibited no subjective expectation of privacy to the exterior of his vehicle because "he did not take any steps to shield or hide the area from inspection by others." [FN65] The court concluded that there was also no objective expectation of privacy since "the exterior of a vehicle, including its bumper, is open to public view and susceptible to casual inspection by the passerby." [FN66] Therefore, under the Nevada Constitution, Nevada law enforcement agents may attach and monitor a GPS device to a vehicle without a warrant.

2. States Where A Warrant is Required

a. Louisiana

The First Circuit Court of Appeal of Louisiana considered the government's use of electronic surveillance "beepers" on the defendants' vehicles in State v. Peters. [FN67] In Peters, law enforcement suspected the defendants of burglaries and obtained a warrant to install and monitor a tracking device on the defendants' vehicles. [FN68] The Court stated that the Louisiana Constitution provides "greater protection for individual rights than that provided by the Fourth Amendment." [FN69] The court noted that any threats to "privacy interests are reasonably protected by obtaining a warrant." [FN70] Therefore, Louisiana law enforcement officials are required to obtain a warrant prior to placing a tracking device on a suspect's vehicle.

***484** b. Oregon

The Supreme Court of Oregon considered the warrantless use of a GPS tracker in State v. Campbell. [FN71] In Campbell, Oregon law enforcement suspected that the defendant was committing residential burglaries. [FN72] Police attempted to follow the defendant's automobile but were unable to do so without detection because of the rural nature of the area. [FN73] Officers then attached a radio transmitter to the underside of the defendant's vehicle while it was parked in a public parking lot. [FN74] Seven days later, officers used the tracking device to discover that the defendant's vehicle was forty miles away. [FN75] Officers used an airplane and visu-

ally observed the defendant getting out of his vehicle and acting in a manner that suggested he was burglarizing a nearby residence. [FN76]

The Supreme Court of Oregon concluded that attaching the transmitter to the defendant's vehicle constituted a "search" under the Oregon Constitution. [FN77] The Court noted that the privacy protected by the Oregon Constitution "is not the privacy that one reasonably expects but the privacy to which one has a right." [FN78] The Court reasoned that the critical question "is whether under our system of government . . . we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement." [FN79] The Court rejected adopting the standard of "public thoroughfares" stated by the United States Supreme Court in Knotts:

> ***485** The argument is factually unsound on the record before us, because the police, notwithstanding diligent efforts, found it impossible to follow defendant's automobile through visual surveillance. . . . Using the transmitter, police were able to locate defendant's automobile some 40 miles from where they expected to find it, and to do so they did not need to maintain constant surveillance of the transmitter or to follow a trail, as one would track a person by looking for footprints, broken branches, etc. [FN80]

The Court, instead, stated that a privacy interest under the Oregon Constitution was "an interest in freedom from particular forms of scrutiny." [FN81] The proper test under the Oregon Constitution is deciding "whether the practice, if engaged in wholly at the discretion of the government, will significantly impair 'the people's freedom from scrutiny, for the protection of that freedom is the principle that underlies the prohibition on 'unreasonable searches."' [FN82]

The Court concluded "any device that enables the police quickly to locate a person or object anywhere within a 40-mile radius, day or night, over a period of several days, is a significant limitation on freedom from scrutiny." [FN83] The fact that there would be no means for individuals to ascertain when they were being scrutinized and when they were not, constituted a staggering limitation upon personal freedom. [FN84] Therefore, under the Oregon Constitution, Oregon law enforcement must obtain a warrant prior to attaching a GPS unit to a suspect's vehicle. [FN85]

***486** c. Washington

The Washington Supreme Court considered whether a warrant was needed for the use of a GPS tracker in State v. Jackson. [FN86] In Jackson, police suspected a father in the disappearance and murder of his daughter. [FN87] Police obtained a warrant to attach a GPS unit to the defendant's vehicle in the belief that the defendant would lead them to his daughter's body. [FN88] The GPS data showed that the defendant went to a remote location where his vehicle remained for about thirty minutes. [FN89] Investigators went to this location and discovered his daughter's body in a shallow grave. [FN90]

On appeal from a guilty verdict for first degree murder, the Supreme Court of Washington considered the use of the GPS tracker in light of the Washington Constitution. The Court held that the Washington Constitution is more protective than the United States Constitution and "focuses on 'those privacy interests which citizens of this state have held, and should be entitled to hold, safe from governmental trespass."' [FN91] The Court stated that no search occurs where a law enforcement officer is able to detect something at a lawful vantage point. [FN92] "However, a substantial and unreasonable departure from a lawful vantage point, or a particularly intrusive method of viewing, may constitute a search." [FN93] Furthermore, "the nature and extent of information obtained by the police . . . is relevant in deciding whether an expectation of privacy an individual has is one which

a citizen of this state should be entitled to hold." [FN94]

***487** The Court concluded that the Washington Constitution required law enforcement to obtain a warrant before attaching a GPS unit to a suspect's vehicle: "[i]f police are not required to obtain a warrant under [the Washington Constitution] before attaching a GPS device to a citizen's vehicle, then there is no limitation on the State's use of these devices on any person's vehicle, whether criminal activity is suspected or not." [FN95] Therefore, under the Washington Constitution, Washington law enforcement officials must obtain a warrant prior to attaching a GPS unit to a suspect's vehicle. [FN96]

3. States Where the Matter is Still In Dispute

a. New York

New York provides a unique situation. Two New York courts of equal authority have considered the issue, but reached opposite conclusions. The New York Nassau County Court first considered the issue in People v. Lacey. [FN97] In Lacey, police investigating a robbery were given a description of the getaway vehicle, including the license plate number. [FN98] Investigators obtained the address of the vehicle's registrant and placed a GPS unit on the vehicle while it was parked on the street. [FN99] Investigators used the GPS signal and visual surveillance to catch the defendant in the process of burglarizing homes. [FN100]

The Nassau County Court considered the activity "a search and seizure" under the New York Constitution:

> [I]ndividuals must be given the constitutional protections necessary to their continued unfettered freedom from a 'big brother' society. . . . [A] person must feel secure that his or her every movement will not be tracked except upon a ***488** warrant based on probable cause establishing that such person has been or is about to commit a crime. . . . [I]t is clear 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 without either the owner's consent or without a warrant issued by a Court. [FN101]

Therefore, the Court concluded that the attachment of a GPS unit to a vehicle without a warrant violated the New York Constitution. [FN102]

The New York County Court for Westchester County also considered the issue in People v. Gant. [FN103] In Gant, the defendant was indicted for criminal possession of a controlled substance. [FN104] The defendant moved to suppress the evidence on the grounds that law enforcement violated the New York Constitution when they attached a GPS unit to his RV without a warrant. [FN105] The Court applied a two-part test measuring first, the defendant's subjective expectation of privacy, and second, the objective expectation of privacy from society's perspective. [FN106] The Court noted that the defendant did not have a reasonable expectation of privacy since he did not own the vehicle. [FN107] The Court then relied on Knotts, stating that there was no reasonable expectation of privacy in the movements of the vehicle. [FN108] The Court concluded that the defendant "has not established that he has a legitimate expectation of privacy in a vehicle traveling upon a public roadways [sic] such that law enforcement was required to obtain a ***489** search warrant prior its installation of a GPS device to track the vehicles' whereabouts." [FN109]

Even though it is unclear from the judicial decisions whether New York law enforcement agents must obtain a warrant before tracking a suspect, the holding in Gant is better reasoned and more persuasive than the holding

in Lacey. Article 1, Section 12 of the New York Constitution guarantees "the right of the people to be secure against unreasonable interception of telephone and telegraph communications." The Lacey Court seems to be relying on this provision when interpreting the reasonableness of the use of GPS by the government, which is technically unrelated to the interception of a telephone or telegraph signal.

The Lacey Court also considered several cases that have examined the issue of GPS use by the government when construing the meaning of the privacy clause in the New York Constitution. [FN110] The Gant Court, however, relied strictly on the precedent of Knotts and construed the privacy clause of the New York Constitution to match the Fourth Amendment to the United States Constitution. Therefore, if the issue were ever to come before a higher New York State court, that court should find that the New York Constitution does not require New York law enforcement agents to obtain a warrant prior to attaching a GPS device to a suspect's vehicle.

III. Alternative Method of Tracking Cellular Phones

The most precise method of tracking individuals is through GPS. GPS can be used to track individuals in their vehicles and through cellular phones. However, GPS is not the only method for tracking cellular phones. Cellular phones can also be tracked when calls are made with the phone through the service provider's cell towers, or cell sites. A cellular phone can be located through signal triangulation when a cell phone "sees" two or more towers. [FN111] Triangulation is easy where cell sites overlap, particularly in high-density population urban ***490** areas. [FN112] In rural areas, the location of a cellular phone often may not be able to be determined as accurately, specifically where cell sites do not overlap and it is not possible to triangulate the signal. However, it is possible to determine the general location of the cellular phone based on the maximum range of the cell site. [FN113]

Government access to location information available through the use of cellular phones is governed by the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"). [FN114] CALEA requires a telecommunications carrier to enable the government, pursuant to a court order, to access "call-identifying information . . . before, during, or immediately after the transmission of a wire or electronic communication." [FN115] "Call-identifying information" is defined 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." [FN116] However, when law enforcement agents only obtain court orders for pen registers and trap and trace devices, [FN117] "such call-identifying information shall not include any information that may disclose the physical location of the subscriber." [FN118]

The FCC, in interpreting and enforcing this statute, however, has found that "a subject's cell site location at the beginning and end of a call is call-identifying information under CALEA." [FN119] Therefore, government agents may obtain only the general cell site location ***491** information of a subscriber. However, in order to obtain information on cell site location, the government must show probable cause that the location information sought is itself evidence of a crime, not that it is relevant to an investigation. [FN120]

It is unclear how the use of GPS in cell phones affects this process. The primary issue is whether court orders for pen registers also permit government officials to obtain GPS location information. The reason for concern is that a different standard could apply to government officials seeking location information. An application for a pen register must certify "that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted." [FN121] If CALEA were construed narrowly to apply only to phone calls, then the use of the GPS service falls out of the scope of the statute and a subscriber's location may not be obtained by

law enforcement through the use of GPS. However, if the statute were applied broadly so that a subscriber's use of GPS qualifies as "call-identifying information," the government fares no better. The location information provided by GPS would fall into the exception that "such call-identifying information shall not include any information that may disclose the physical location of the subscriber" and would still not be available to the government. [FN122]

On the face of the statute, a subscriber's physical location is protected from being released to the government upon the filing of an application for a pen register. One federal court has authorized government officials to obtain cell-site location information while denying detailed triangulation or GPS location information, pursuant to a pen register application upon a showing that the information was likely relevant to an ongoing investigation. [FN123] These statutes, however, apply only to the real-time tracking of a suspect through his cell phone. Would a service provider's records of a subscriber's use of a GPS service through his cell phone be equally off limits to law enforcement agents?

***492** IV. Government Access to Records Regarding Location

The government has the power not only to track the location of a suspect's vehicle or cellular phone in real time, with the appropriate legal process, but also can access any records of a suspect's location kept by a third-party service provider. The seminal case regarding the government's access to records is United States v. Miller. [FN124] In Miller, the defendant was convicted of possessing an unregistered whiskey still with the intent to defraud the government of the whiskey tax. [FN125] During the investigation, agents from the Alcohol, Tobacco and Firearms Bureau presented subpoenas for all of the bank records of the defendant to the presidents of the banks where the defendant held accounts. [FN126] The banks did not notify the defendant about the subpoenas but instead gave the documents to the government agents. [FN127] The bank records were then presented to a grand jury and the grand jury returned an indictment of the defendant. [FN128]

The Supreme Court of the United States held that there was "no intrusion into any area in which respondent had a protected Fourth Amendment interest." [FN129] The Court held that the defendant had no ownership or possessory interest in the documents because they were the business records of the bank. [FN130] Because all of the documents contained information voluntarily conveyed to the banks, 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." [FN131] The Court stated the rule broadly:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to ***493** Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed. [FN132]

Therefore, the government may obtain any collected information from a third party without violating the Fourth Amendment.

Congress restricted the holding in Miller by requiring government officials seeking financial records to serve a copy of the subpoena on the customer and by requiring customers who wish for their records to remain private to file a motion to quash within ten days of service or risk waiving protection of their bank records. [FN133] Many privacy advocates are also critical of the holding in Miller. One critic urges that "the individual's intent in disclosing the record at issue to the business is critical in determining whether such disclosure should be considered 'voluntary.'" [FN134] Another critic argues that a broad reading of Miller should be rejected because a

holding that "any reliance on a third party to retain a communication eliminates an expectation of privacy in the contents of the communication is inconsistent with Katz." [FN135]

The Miller ruling merits clarification. Under Miller, third-party documents may be disclosed pursuant to a subpoena duces tecum. [FN136] A subpoena is issued by an attorney, who acts as a representative of the court. [FN137] Third-party documents are subject to a subpoena if they are likely to lead to relevant evidence. [FN138] A subpoena is therefore different from a warrant. A warrant is an order that is issued by the judge that authorizes a law enforcement officer to search for and seize ***494** any property that constitutes evidence of the commission of a crime. [FN139] Therefore, as a result of this distinction, a warrant from the judge is required to allow the government to directly track a suspect with a GPS unit while only a subpoena is required to allow the government to obtain documents containing relevant location information from GPS service providers.

Applying Miller to business records of GPS vehicle location, the government has no limitation in accessing information of a person's location that is kept by the service provider. A court could find that a person voluntarily conveyed his location to a service provider by subscribing to a GPS based service when the subscriber has the knowledge that the provider will have access to his location information. The amount of information that the government can collect in this indirect manner is limited only by the amount and detail of the records kept by the service providers. According to OnStar's Privacy Policy:

> OnStar only knows where your car is when a user or subscriber initiates a request for service, there is an Air Bag Deployment, an Advanced Automatic Crash Notification occurs, or OnStar is required to locate the car to comply with legal requirements, including valid court orders showing probable cause in criminal investigations. [FN140]

Therefore, law enforcement officials would be able to access any records of a customer's vehicle location only when the customer was using the service, such as obtaining driving directions, or when the GPS equipment automatically calls the service provider for software updates.

The amount of location information available to law enforcement through GPS service providers like OnStar may be severely limited. While OnStar is available on over fifty models of GM's 2007 line, [FN141] OnStar is not able to track all of these vehicles. [FN142] Vehicles for which ***495** the service is not purchased are deactivated and are unable to be tracked by OnStar. [FN143] Also, when a subscriber of OnStar makes a request for service, OnStar has location information of the vehicle only for the time of the communication transmission. [FN144] Once the communication transmission is terminated, OnStar no longer has any GPS location information on the vehicle. [FN145] For instance, if a subscriber contacts OnStar with a request for driving directions, OnStar only has the location information of the vehicle during the time that the directions are transmitted to the vehicle and does not know the location of the vehicle as it follows those directions.

Furthermore, Miller would also seem to apply to the use of GPS-based services in a subscriber's cell phone. Any records kept by a service provider of a subscriber's location would seem to be available to government agents on the grounds that the subscriber voluntarily conveyed his location to the service provider and took the risk that the information would be conveyed to the government.

V. Conclusion

There seems to be ample protection in place for consumers' privacy concerns regarding government access to location information. When a person uses a vehicle, its location information is open to public scrutiny. The

vehicle may be observed by anyone. The fact that federal law enforcement may use GPS tracking devices without a warrant does not infringe on the privacy of a person any more than if federal agents were to visually tail the vehicle. State law enforcement agents are limited by their respective state constitutions, and only Louisiana, Oregon, and Washington have reached the conclusion that law enforcement agents must obtain a warrant prior to attaching a GPS unit to a suspect's vehicle.

The only restriction placed on law enforcement by the Fourth Amendment is that agents must not pass the curtilage of a residence to attach a GPS unit to a suspect's vehicle, such as if the vehicle were parked in the suspect's garage. However, this limitation is irrelevant as most people who drive vehicles eventually park them in public locations. Law enforcement agents only need to wait for the suspect to park the vehicle in a public location to attach the GPS unit to the ***496** vehicle. The federal courts, and half of the state courts to consider the issue, have found no constitutional protection afforded to citizens from the government use of GPS.

As for records of vehicle location kept by a service provider, the subscriber is voluntarily conveying his location information to the service provider and is taking the riskthat those records may be obtained by the government pursuant to a subpoena. This would likely be the case, because subscribing to GPS location service is not a necessity to the extent that a bank account is under Miller. If a customer does not want to risk that records of his location at a few specific instances will be subject to a subpoena from the government, then the customer can simply choose not to purchase the service. This history of location information is limited only by the detail of the service provider's records and the length of time for which the records are kept.

This level of protection also seems ample to protect a consumer's location information that would be available through the use of a cellular phone. When law enforcement officials obtain a warrant for a pen register, they are limited to the location of the cell site. This only gives a general location of the suspect and is not as intrusive as the use of a GPS unit on a suspect's vehicle. If government agents were to obtain a warrant to track a suspect through the GPS unit in his cellular phone, agents would have access to the specific location of a suspect. However, since people mainly use cellular phones when they are in public, there would be no violation of a person's Fourth Amendment rights. Because the person is out in public, there would not be a reasonable expectation of privacy. The only situation where the Fourth Amendment would be violated is if law enforcement agents were to track a suspect's cellular phone through its GPS unit without a warrant and the suspect was located in his house at the time of the tracking. According to the Supreme Court's analysis in Kyllo, this situation would result in an unreasonable search.

There are two reasons, however, why this situation would likely never arise. The first is that the technology is limited. It is not possible to get signals of GPS units indoors. “Because the phone picks up GPS signals from satellites like other satellite systems (DirectTV for instance), it won't be able to get positions while being indoors, underground or in tunnels.” [FN146] Therefore, even if law enforcement attempted to track the GPS unit in a cellular phone, there would be no ***497** location information available as long as the cellular phone is in a building, including a private residence.

The second reason why this situation would not arise is that service providers are not likely to voluntarily hand over a subscriber's location information to law enforcement agents without a warrant. “The theory holds that the marketplace will protect privacy because the fair treatment of personal information is valuable to consumers; in other words, industry will seek to protect personal information to gain consumer confidence and maximize profits.” [FN147] For instance, Verizon Wireless “always requires a warrant from law enforcement officials.” [FN148] It would only take one high-profile case of bad publicity to hurt a service provider's standing in

the market. To prevent this, service providers are likely to always require a warrant from law enforcement officials before tracking a suspect's GPS unit in his cellular phone.

It is apparent that citizens are provided ample protection from government intrusion when the government decides to track a suspect's location through the use of GPS. Citizens are protected in private spaces by the Fourth Amendment, by physical limitations on the technology, and by market pressures. Whether more stringent protections from GPS tracking by the government should be guaranteed to citizens while in public space is a determination to be made by Congress.

[FNa1]. The author is a 2008 J.D. candidate at The Ohio State Moritz College of Law. He received a B.S. in Biology from The University of Akron in 2001.

[FN1]. See National Parks Service, The History of GPS, http:// www.nps.gov/gis/gps/history.html (last visited Dec. 30, 2007).

[FN2]. See Scott Pace et al., The Global Positioning System: Assessing National Policies 237-38 (1995), http://www.rand.org/pubs/monograph_ reports/MR614/MR614.appb.pdf.

[FN3]. For an explanation on the process of how GPS works, see Trimble, GPS Tutorial, http://www.trimble.com/gps/howgps.shtml (last visited Dec. 30, 2007).

[FN4]. See OnStar by GM, OnStar & GPS Equipped Vehicles, Auto Navigation System, http://www.onstar.com/us_english/jsp/equip_vehicles/07_vehicles.jsp (last visited Dec. 30, 2007).

[FN5]. See Verizon Wireless, Point Yourself in the Right Direction with VZ Navigator, http://www.verizonwireless.com/b2c/splash/turnbyturn.jsp (last visited Dec. 30, 2007).

[FN6]. 47 C.F.R. § 20.18 (2006).

[FN7]. Id.

[FN8]. See Geoffrey D. Smith, Private Eyes Are Watching You: With the Implementation of the E-911 Mandate, Who Will Watch Every Move You Make?, 58 Fed. Comm. L.J. 705, 706 (2006) ("In 2001, a thirty-two year old woman drove off of the Florida Turnpike, into a canal. As her car was sinking she dialed 911. She talked to the dispatcher for over three minutes but did not know her exact location. Rescuers were unable to find her before she died.").

[FN9]. Retention of Telephone Toll Records Rule. 47 C.F.R. § 42.6 (2006) ("Each carrier that offers or bills toll telephone service shall retain for a period of 18 months such records as are necessary to provide the following billing information about telephone calls: the name, address, and telephone number of the caller, telephone number called, date, time and length of the call.").

[FN10]. A related issue to privacy of information in the use of vehicles is the use of event data recorders, or automobile "black boxes." However, this article will focus specifically on privacy in location information. Event data recorders do not record location information, but instead only record performance information of the vehicle such as speed, braking power, and seat belt use. See W.R. Haight, Automobile Event Data Recorder

(EDR) Technology-Evolution, Data, and Reliability (2001), available at http://www.accidentreconstruction.com/research/edr/docs/EDRPaperRHaight.pdf. Therefore, automobile event data recorders fall outside of the scope of this article.

[FN11]. U.S. Const. amend. IV.

[FN12]. John S. Ganz, Comment, It's Already Public: Why Federal Officers Should Not Need Warrants to Use GPS Vehicle Tracking Devices, 95 J. Crim. L. & Criminology 1325, 1332 (2005) (citing United States v. Jacobsen, 466 U.S. 109, 113 (1984)).

[FN13]. Id. at 1333 (citing United States v. Bailey, 628 F.2d 938, 945 (6th Cir. 1980)).

[FN14]. Id. (citing Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 450 (1990)).

[FN15]. United States v. Knotts, 460 U.S. 276 (1983).

[FN16]. United States v. Karo, 468 U.S. 705 (1984).

[FN17]. Kyllo v. United States, 533 U.S. 27 (2001).

[FN18]. United States v. Moran, 349 F. Supp. 2d 425 (N.D.N.Y. 2005).

[FN19]. Knotts, 460 U.S. at 278.

[FN20]. Id.

[FN21]. Id.

[FN22]. Id.

[FN23]. Id. at 279.

[FN24]. Id.

[FN25]. Id.

[FN26]. Id. at 285.

[FN27]. Katz v. United States, 389 U.S. 347, 361 (1967).

[FN28]. Knotts, 460 U.S. at 280-81.

[FN29]. Id. at 281. The Court explained this diminished expectation of privacy in an automobile by stating: “One 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. A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view.” Id. (citing Cardwell v. Lewis, 417 U.S. 583, 590 (1974)).

[FN30]. Knotts, 460 U.S. at 285.

[FN31]. Id.

[FN32]. Karo, 468 U.S. 705.

[FN33]. Id. at 708.

[FN34]. Id.

[FN35]. Id. at 709.

[FN36]. Id. at 709-10.

[FN37]. Id. at 710.

[FN38]. Id. at 714.

[FN39]. Id.

[FN40]. Kyllo, 533 U.S. 27.

[FN41]. Id. at 29.

[FN42]. Id. at 29-30.

[FN43]. Id. at 30.

[FN44]. See id. at 40.

[FN45]. Id.

[FN46]. Moran, 349 F. Supp. 2d 425.

[FN47]. Id. at 467.

[FN48]. Id.

[FN49]. Id.

[FN50]. Osburn v. State, 44 P.3d 523, 525 (Nev. 2002) (citing Michigan v. Long, 463 U.S. 1032, 1041 (1983)).

[FN51]. People v. Zichwic, 114 Cal. Rptr. 2d 733 (Cal. Ct. App. 2002).

[FN52]. Id. at 737.

[FN53]. Id.

[FN54]. Id. at 737-38.

[FN55]. Id. at 743.

[FN56]. Id. at 739.

[FN57]. Id. at 742.

[FN58]. Id. at 743.

[FN59]. Id.

[FN60]. Osburn, 44 P.3d 523.

[FN61]. Id. at 524 (the defendant's vehicle was parked on the street at the time the monitoring device was attached).

[FN62]. Id.

[FN63]. Id.

[FN64]. Id. at 526.

[FN65]. Id.

[FN66]. Id. (“Moreover, manufacturers, dealers and owners often take advantage of this public visibility by displaying model names, company logos, decals, and bumper stickers on the exteriors of automobiles. In light of these facts, we can see no objective expectation of privacy in the exterior of an automobile.”).

[FN67]. State v. Peters, 546 So. 2d 829 (La. Ct. App. 1989).

[FN68]. Id. at 833.

[FN69]. Id. at 834.

[FN70]. Id.

[FN71]. State v. Campbell, 759 P.2d 1040 (Or. 1988).

[FN72]. Id. at 1041.

[FN73]. Id.

[FN74]. Id. at 1042.

[FN75]. Id.

[FN76]. Id.

[FN77]. Id. at 1041.

[FN78]. Id. at 1044.

[FN79]. Id. (citations omitted).

[FN80]. Id. at 1045.

[FN81]. Id. at 1047.

[FN82]. Id. at 1048.

[FN83]. Id. (“The limitation is made more substantial by the fact that the radio transmitter is much more difficult to detect than would-be observers who must rely upon the sense of sight. Without an ongoing, meticulous examination of one's possessions, one can never be sure that one's location is not being monitored by means of a radio transmitter.”).

[FN84]. Id. at 1049.

[FN85]. The Oregon Supreme Court revisited the issue in State v. Meredith, 96 P.3d 342 (Or. 2004). The United States Forest Service (“USFS”) suspected the defendant, an employee of USFS, of arson. Id. at 343. USFS attached a GPS unit to the undercarriage of the vehicle (owned by USFS) used by the defendant and used it to catch defendant in the act of arson. Id. The Court concluded that the “defendant did not have a protected privacy interest in keeping her location and work-related activities concealed from the type of observation by her employer that the transmitter revealed.” Id. at 346.

[FN86]. State v. Jackson, 76 P.3d 217 (Wash. 2003).

[FN87]. Id. at 220.

[FN88]. Id. at 221.

[FN89]. Id.

[FN90]. Id.

[FN91]. Id. at 222.

[FN92]. Id.

[FN93]. Id. (citations omitted).

[FN94]. Id.

[FN95]. Id. at 224.

[FN96]. In Jackson, the Court affirmed the conviction because law enforcement had obtained warrants prior to attaching the GPS device, and because the warrants were supported by probable cause. Id. at 227.

[FN97]. People v. Lacey, 2004 WL 1040676 (Nassau County Ct. 2004).

[FN98]. Id. at *1.

[FN99]. Id.

[FN100]. Id. at *2.

[FN101]. Id. at *7-8.

[FN102]. However, because the defendant did not own the vehicle, he did not have standing to assert that his rights were violated under the New York Constitution. Therefore, his motion to suppress the evidence was denied. Id. at *9-10.

[FN103]. People v. Gant, 802 N.Y.S.2d 839 (Westchester County Ct. 2005).

[FN104]. Id. at 840.

[FN105]. Id. at 845.

[FN106]. Id. at 845-46 (stating that "Where there is no expectation of privacy, there is no search and seizure.") (citations omitted).

[FN107]. Id. at 845.

[FN108]. Id. at 846.

[FN109]. Id. at 847. "In addition, this Court finds 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." Id. The court further held that its decision was consistent with Lacey since the defendants in both cases lacked standing. Id. at 848.

[FN110]. See Lacey, 787 N.Y.S.2d at *4-7.

[FN111]. Recent Development, Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators. 18 Harv. J.L. & Tech. 307, 308 (2004).

[FN112]. See Wikipedia, Cell Site, http://en.wikipedia.org/wiki/Cell_site (last visited Dec. 30, 2007).

[FN113]. Id. (The maximum range of a cell site where the terrain is flat is between 50 to 70 kilometers. The maximum range of a cell site where the terrain is hilly can vary from 5 to 40 kilometers.).

[FN114]. 47 U.S.C. §§ 1001 et seq. (2006).

[FN115]. 47 U.S.C. § 1002(a)(2)(A) (2006).

[FN116]. § 1001(2).

[FN117]. These are methods of obtaining call information such as routing, numbers called by the subscriber, or numbers of incoming calls, but not the actual content of the call. See 18 U.S.C. § 3127 (2006).

[FN118]. 47 U.S.C. § 1002(a)(2)(B) (2006).

[FN119]. FCC, In re Communications Assistance for Law Enforcement Act, 14 F.C.C.R. 16794, ¶ 44 (1999) ("Third Report and Order"). This interpretation was upheld in U.S. Telecomm. Ass'n v. FCC, 227 F.3d 450 (D.C. Cir. 2000).

[FN120]. See In re Order Authorizing the Release of Prospective Cell Site Information, 407 F. Supp. 2d 134 (D.C. Cir. 2006).

[FN121]. 18 U.S.C. § 3122(b)(2) (2006).

[FN122]. § 1002(a)(2)(B).

[FN123]. See In re Order Authorizing the Installation and Use of a Pen Register, 411 F. Supp. 2d 678 (W.D. La. 2006).

[FN124]. United States v. Miller, 425 U.S. 435 (1976).

[FN125]. Id. at 436.

[FN126]. Id. at 437.

[FN127]. Id. at 438.

[FN128]. Id.

[FN129]. Id. at 440.

[FN130]. Id.

[FN131]. Id. at 443.

[FN132]. Id.

[FN133]. 12 U.S.C. § 3405 (2006).

[FN134]. Deidre K. Mulligan, Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 Geo. Wash. L. Rev. 1557, 1581 (2004).

[FN135]. Patricia L. Bellia, Surveillance Law through Cyberlaw's Lens, 72 Geo. Wash. L. Rev. 1375, 1405 (2004).

[FN136]. A subpoena duces tecum is a writ ordering a witness to appear and produce documents. Black's Law Dictionary 674 (2d Pocket ed. 2001).

[FN137]. Fed. R. Civ. P. 45(a).

[FN138]. See Fed. R. Civ. P. 26(b).

[FN139]. New Jersey Library Ass'n, Guidelines to Assist Libraries with Requests for Confidential Library Records, (2002), http:// www.njla.org/statements/confoflib.html.

[FN140]. OnStar, OnStar Privacy Statement, July 2007, http:// www.onstar.com/us_english/jsp/privacy_policy.jsp.

[FN141]. See OnStar by GM, supra note 4.

[FN142]. Telephone Interview with Joanne Finnorn, General Counsel, OnStar (Dec. 21, 2006).

[FN143]. Id.

[FN144]. Id.

[FN145]. Id.

[FN146]. AccuTracking, Frequently Asked Questions, http:// support.accutracking.com/index.php?x=&mod_id=2&root=2 (last visited Dec. 30, 2007).

[FN147]. Joel R. Reidenberg, Restoring Americans' Privacy in Electronic Commerce, 14 Berkeley Tech. L.J. 771, 774 (1999).

[FN148]. Telephone Interview with Jeffrey Nelson, Public Policy and Regulatory Affairs Spokesman, Verizon (Nov. 16, 2006).
3 I/S: J. L. & Pol'y for Info. Soc'y 473

END OF DOCUMENT