JICLT
Journal of International Commercial Law and Technology
Vol. 8, No.1 (2013)

Warrantless GPS Tracking: Who Cares About Vehicle Transponders – What About Your Cell Phone ?

Eric Samuel Heidel*

ericheidel@att.net

Abstract: The government now regularly gathers information from individuals' smartphones. Cellular providers are allowing the government to access the GPS data that users' smartphones exchange with the provider. While there are legitimate purposes for this disclosure without the consent of the smartphone user, there are many instances were no emergency situation exists and no search warrant is even sought. The law currently views sharing GPA data with a cellular provider as a voluntarily disclosure, creating a lesser expectation of privacy. Although posting locations on social networking sites is a clear public disclosure, using modern technology for directions or other conveniences should not cause an individual to forfeit privacy.

.

1. Introduction

The Supreme Court recently released its highly anticipated decision in United States v. Jones, holding that placing a Global Positioning System ("GPS") tracker on a private vehicle is a search within the meaning of the Fourth Amendment of the Constitution. Only a few decades ago, this issue would have been beyond anyone's imagination. Lower courts and even the Supreme Court have found previous Fourth Amendment decisions to be of little help in the quickly advancing technological world of the twenty-first century.

More specifically, the Court has been presented with several cases involving tracking devices. It began with beacons that emitted a signal up to a certain distance, and most recently, in Jones, the Court dealt with placing GPS transponders on vehicles. Before the late twentieth century, police would simply follow a suspect on public thoroughfares. This surveillance technique did not implicate any constitutional protections since police were on public streets, and Supreme Court "cases suggest that such visual observation is constitutionally permissible."

Traditional surveillance "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance." Unlike the current situation where a small GPS device is largely undetectable, private citizens could previously, with relative ease, determine if law enforcement was following them. GPS trackers are controversial because without inspecting the entire vehicle, undercarriage and all, before each outing, the common citizen is unlikely to be aware of the device and subsequent tracking. However, now that "GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.' "

Tracking smartphones is far more practical than tracking vehicles with transponders attached; that is, the average person is unlikely to ever leave his or her phone behind. Americans wear their phones on their arms when they run or walk, bring them along when traveling by car, bus or train, and otherwise have them in a pocket, coat, or bag on their person. In fact, "as of June 2011… there were more than 322 million wireless devices in use in the United States."

The central issue is whether the police can track the GPS built into a smartphone without a warrant. The underlying question is whether the tracking of the GPS location of a smartphone is even a search at all. The first part of this article explores the Fourth Amendment to the United States Constitution and the relevant search and seizure jurisprudence of the United States Supreme Court. The second part delves into the Katz reasonable expectation of privacy test that the concurring Justices indicate is most appropriate for future cases that do not involve a physical intrusion of any kind, as is the case with the built-in GPS transponders of smartphones. The third section addresses the limitations that the Court's

recent decision in the Jones case has placed upon the use of GPS tracking. Last, the fourth section discusses the reality that smartphone users voluntarily provide GPS location data to a third party and the implications sharing that information has on a user's expectation of privacy.

Technological advances threaten the Fourth Amendment protection of citizens from government searches and seizures by creating a culture of trading privacy for modern conveniences, which require sharing information with remote servers maintained by third parties. In order to deem tracking the GPS location of a smartphone a search and thus require a warrant, the Court must narrow the implications of sharing information with a third party to exclude the automated sharing of technical information with the provider of a service that cannot function without such information. Americans should not be required to forego privacy rights in order to use modern and readily available technologies to improve their lives.

2. The Fourth Amendment- It protects us, but is it even a true barrier to government Intrusion when it comes to GPS?

In the Jones case, the Court held that "[i]t may be that achieving the same result [as traditional surveillance] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question." The Court made reference to the very circumstances created when addressing GPS in smartphones. Justice Sotomayor went a step further in observing that a "physical intrusion is now unnecessary to many forms of surveillance." Justice Sotomayor went on to note, "the Government will be capable of duplicating the monitoring undertaken in [the Jones case] by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones." Partial exploration of Fourth Amendment doctrine is necessary before delving into the looming uncertainty regarding the Fourth Amendment's restraints on new technologies like smartphones.

Essentially, the Fourth Amendment protects individuals from the whims of the government when it comes to searches and seizures. While the search language may seem to be the more simple of the two, the Court has created several exceptions over the last half century. Seizures seem almost synonymous with arrest, but it is not quite that simple. For instance, the traditional exigent circumstances do not exist because there is no search; these exceptions simply allow for government to search without a warrant. Justice Douglas, some forty years ago, made the same point:

> "There is, so far as I understand constitutional history, no distinction under the Fourth Amendment between types of crimes. Article III, s 3, gives 'treason' a very narrow definition and puts restrictions on its proof. But the Fourth Amendment draws no lines between various substantive offenses. The arrests on cases of 'hot pursuit' and the arrests on visible or other evidence of probable cause cut across the board and are not peculiar to any kind of crime. I would respect the present lines of distinction and not improvise because a particular crime seems particularly heinous. When the Framers took that step, as they did with treason, the worst crime of all, they made their purpose manifest."

This is brilliance embedded into logic. The Framers explicitly enunciated a crime that was to be dealt with in a different manner right in the Constitution. Therefore, one can infer that all other crimes are to be addressed using the traditional constitutional framework, of which the Fourth Amendment is a crucial part.

Of concern are those searches of smartphones that users may not be aware of. They do not witness government take physical custody of their phone and search through it. Police should not be able to remotely access the contents of, more specifically the GPS locator in, a person's smartphone without a warrant or consent. However, if a person consents to having their phone tracked, the purpose of the tracking will be defeated since the person will be aware of the GPS tracking and perhaps alter his activities.

The issue is whether accessing the built-in GPS tracker on a smartphone is even a search. If it is not a search, then there is no Fourth Amendment protection afforded. The Jones case laid the groundwork when the majority held that "the Government's installation of a GPS device on a target's vehicle, and its

use of that device to monitor the vehicle's movements, constitutes a 'search.' " With a showing of probable cause and a search warrant issued, the government could obtain GPS tracking data.

While installing a GPS device and using it to monitor movement is a search, there is still uncertainty as to whether there is a search when there is no installation of a GPS transponder and thus no corresponding physical intrusion. The Court itself admits that in some instances there is no seizure even when there is an installation since "some meaningful interference with an individual's possessory interests in that property" would have had to occur. The installation and monitoring of a GPS transponder on a vehicle, alone, causes no such interference with the operation of vehicle. However, there could be a seizure without any installation or actual physical occupation.

Smartphone users can attest to the fact that using the GPS on their phone for things such as an application that provides driving directions causes a significant drain on the battery. A person undoubtedly has a possessory interest in the battery in his own smartphone. The phone only functions if the battery is charged and operational. Draining that battery by using a person's built-in GPS could be interpreted as a meaningful interference under the language in Jacobsen. Technically, monitoring a person's GPS deprives that person of the ability to use that portion of their battery that has been drained. It is not hard to foresee, in such a litigious society, an individual who files suit when he is unable to call 911 in an emergency situation because his battery was significantly drained by government tracking his GPS location. But for government's warrantless use of the GPS, that person would have enough battery to call for help.

When government installs its own transponders on cars, the batteries have to be replaced. It would be impossible for government to contend that it does not interfere with the battery life by accessing built-in smartphone GPS. Whether using extra battery power constitutes a "meaningful interference" in regards to a smartphone battery is not even something that the Court foresaw eventually having to decide, providing not even a passing reference.

The Court did foresee a future argument that perhaps the use of GPS without a warrant could be allowed if the crime is heinous enough. Certainly government could garner public support if there is a pressing need to use this GPS technology when a killer is on the loose or a child predator escapes. However, the Court held in Jones that "[t]here is no precedent for the proposition that whether a search has occurred depends on the nature of the crime being investigated." Thus, the Court finds that the nature of the crime cannot negate the fact that a search is a search.

While the Supreme Court has recently heard the Jones case involving the antiquated and less effective installation of GPS transponders on vehicles, at least one lower court has heard a case that provides further and more pointed guidance on the matter of smartphones. In re Application of U.S. for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone dealt with "the government's authority to prospectively acquire precise location information derived from cellular and Global Positioning System ("GPS") technology (collectively "location data") to aid in the apprehension of the subject of an arrest warrant." A federal court recently precluded the government from using the GPS in an individual's phone even when there was already an arrest warrant for that person. The government sought "to use [the] location data in a new way—not to collect evidence of a crime, but solely to locate a charged defendant."

This is a powerful decision. A search warrant allows government to search for evidence of a crime after a showing of probable cause to a neutral magistrate. However, an arrest warrant is issued after evidence of a crime has already been discovered. This means that government now has the authority to actually seize this individual and not just search him, his home, or his effects. The inference is that if government cannot use GPS in a smartphone to locate the subject of an arrest warrant, then government cannot use GPS to follow a suspect in order to amass evidence to seek an arrest warrant. The latter is a much less compelling argument than the former of searching for a wanted alleged criminal, yet the former was rejected by a federal court.

This entire topic begs the question: why is it that government will not just get a search warrant? In fact, the government was able to obtain a search warrant in the Jones case. Government just failed to execute the warrant by placing the GPS transponder on the vehicle within the specified time period. To be clear, in that investigation, the need for a search warrant would have in absolutely no way jeopardized the efforts of the police; they were able to obtain one.

Aside from the fact that the search warrant was readily and actually obtained in Jones, the legal standard to be met to obtain a search warrant is relatively low. No court is asking for proof beyond a reasonable doubt or even a preponderance of the evidence in order to issue a search warrant. Courts simply require probable cause to be shown in accordance with the Fourth Amendment. Probable cause

has never been assigned an exact percentage or probability, and there is not a requirement that police be absolutely certain. Police are likely to satisfy a department standard at or above probable cause before expending a large number of resources in an investigation of this sort since there are no criminal penalties for a suspect arrested and charged without complying with constitutional requirements.

Moreover, "Congress and most States have not enacted statutes regulating the use of GPS tracking technology for law enforcement purposes." This is encouraging news for government. Congress and state legislatures could only act to make the requirements for using GPS tracking even more difficult for law enforcement to act to the contrary would be violative of the Fourth Amendment. The standard is at its lowest and yet government has, in numerous instances, failed to even apply it, let alone comply with it. The Court, however, has reined in the use of GPS tracking in the Jones decision and indicated that the use of GPS tracking in some situations does constitute a search. The concurring opinions of Jones are more helpful than the majority decision in situations that do not involve an actual physical intrusion or trespass.

3. Reasonable Expectation of Privacy

The most useful language to come out of the Jones case for situations involving built-in GPS are the references to Katz v. United States; that is, the mention of the reasonable expectation of privacy.

A. The Katz Test

The Katz case sets forth the two-prong test for the reasonable expectation of privacy. The Katz test has been cited throughout modern jurisprudence on matters involving the Fourth Amendment. Justice Sotomayor quotes another recent case, *Kyllo v. United States*, in her Jones opinion when she states that "even in the absence of a trespass, 'a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.' " Now, two twenty-first century Supreme Court cases have cited the rule described in Katz in the 1960's when there was an expansion of privacy interests. The law has evolved so that "there is a twofold requirement, first that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' "

The first part of the test is the subjective expectation; that is, what the person in the particular set of facts expected to be private. It is well settled that "a man's home is, for most purposes, a place where he expects privacy." This is largely due to the nature of a house and the inherent privacy in its design. While this is for the objective prong, society very clearly recognizes the home as a private location with the highest expectation of privacy. To preserve the subjective expectation of privacy one must act in a manner consistent with that expectation. For instance, in the Katz case, law enforcement placed a listening device on a phone booth. The government argued that there was no intrusion into the phone booth and that since it was glass (transparent) and in public, there was no subjective expectation of privacy. The Court found differently and decided that by placing himself in an actual phone booth, there was a subjective expectation of privacy since it was what could be heard that Katz was protecting, and not what could be seen. "On the other hand," … the Court was sure to find that "conversations in the open would not be protected against being overheard." At a broader, more abstract level, "objects, activities, or statements that [a person] exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited." This would mean, for example, that an individual walking around with a clear backpack is displaying no subjective expectation of privacy. An individual with a more traditional black cloth backpack is exhibiting a subjective expectation of privacy.

This brings about the natural next step, the objective prong. Society cannot allow every individual to claim an expectation of privacy in just anything. For example, the Court went on to find that conversations in the open, as opposed to in a phone booth, were not protected "for the expectation of privacy under the circumstances would be unreasonable." The majority in Jones is likely concerned that the objective prong is open to that living, changing, breathing document argument. Nonetheless, the Katz test is good law and the objective prong deals with what society sees as reasonable. Society would not have seen many things that are seemingly innocuous today as such in the 1920's, for example. Society is likely to see having a black cloth backpack as a reasonable subjective showing of privacy and respect that.

Simply showing a subjective intent is not enough. Society must find that expectation of privacy to be reasonable. The Court itself has criticized the Katz test on several occasions as being circular. There is also an argument that it is difficult for judges and justices alike to differentiate between what they see as a reasonable expectation of privacy and what society as a whole finds to be reasonable. This could imply that courts should rely on public polls to gauge what society determines to be reasonable. It would be a rather absurd notion to allow the whims of a public captivated by the likes of reality television to decide the law in this country.

B. How do we show our subjective expectation in today's world?

In the context of technology, it is not as simple as buying a bag that is not transparent to demonstrate a subjective intent to keep something private. For instance, one may text message using his smartphone while in a public park, but have no intent to share what is contained in those text messages with anyone else. Naturally, it follows that text messaging is silent, so he has succeeded from the standpoint that no one else can overhear. But, there remains the question of whether exposing the actual phone itself defeats that expectation of privacy. To answer that, there is some analogous well-settled law, the plain view doctrine. Police are able to use evidence of a crime that they can see in plain view when lawfully occupying an area, whether it be public or private. However, the doctrine falls short of allowing police to even turn over something that is not inherently criminal to investigate further since the object in and of itself does not create probable cause. In contrast, marijuana sitting out on a dining room table, visible as police validly enter a home, is enough to create probable cause since the very possession of marijuana is illegal; that is, possessing that substance is indisputably criminal. A smartphone, or any mobile phone for that matter, is not immediately indicative of criminal wrongdoing. A smartphone's primary and apparent purpose is not criminal. Thus, privately engaging in text messaging or emailing on a smartphone can still maintain that subjective element, even if the actual phone is brandished in public.

The next logical step is to determine how to show a subjective expectation of privacy when government is remotely accessing the phone. In today's world of technology, most smartphones have an option for a passcode. This passcode must be entered in order to access the contents and features of the phone, everything but the ability to make an emergency call. One is hard pressed to think of a clearer way to show that anything that the phone does inside the actual casing is private. Using the passcode demonstrates that even when the phone is not on the person of the owner, the owner does not expect anyone else to be able to access the phone's contents, just as the owner of a debit card does not expect it to be of use, if left out, without the pin number.

The government in the Jones case relied in part on the holding from *United States v Knotts*, in which the Court held that a "person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." This argument may have been plausible, although still discredited, in the case of installing a transponder on a vehicle, but it is a much different situation when tracking a phone. Individuals could be tracked within their home. The GPS could reveal when two people are in bed together, violating the most protected of areas, the bedroom. With cameras everywhere in public places today, the government's argument is by and large applicable for a person walking down the street or that is really anywhere in public.

Can a person have a subjective expectation of privacy when he is in public with cameras all around? That answer is likely no. However, a person could have an expectation of privacy as to what happens within his smartphone. After all, only the shell is visible to those cameras and the public. This logical explanation, however, runs contrary to the law. The Fourth Amendment protects people. While the smartphone is a personal effect, the purpose of requiring a search warrant for tracking the built-in GPS on a smartphone would be to protect the person. When that person is in public with cameras all around and thus has no subjective expectation of privacy, then the person cannot be protected—the GPS location data reveals no more than does the view of the cameras. It is the subjective expectation of privacy when entering one's home or the home of a friend or family member that has the very real potential of being violated if warrantless GPS tracking of smartphones is permitted.

"The critical fact in [the Katz] case is that '(o)ne who occupies it, (a telephone booth) shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume' that his conversation is not being intercepted." This comparison becomes clearer when compared with the idea of stopping on the street to ask someone how to get somewhere as opposed to retaining an expectation of privacy by using the GPS in one's phone. However, that argument might only be valid if there were no

cameras. Even with no cameras, it will still be difficult to argue any expectation of privacy when on public roadways or walkways immediately adjacent to those roadways. Admittedly, there is a higher expectation of privacy in accessing the GPS on one's phone as opposed to asking for directions. Using the GPS as opposed to asking for directions is simply a means to show that one wishes to keep his location private by paying for a more private service, namely the smartphone data plan. However, this is unlikely to succeed in defeating the public thoroughfare language of Supreme Court precedent.

"What mattered … was whether the conduct at issue 'violated the privacy upon which [the defendant] justifiably relied while using the telephone booth.' " Therefore, what matters here is whether tracking a person's smartphone GPS violates his privacy in whatever setting he may be in, and the number of possible settings is certainly greater than those that a vehicle could be found in.

C. Modern Society and the Objective Expectation

Gone are the days when having ownership of land or an object meant that society and the law recognized complete privacy. The Court has indicated that "[t]he premise that property interests control the right of the Government to search and seize has been discredited." The more modern interpretation of property rights is that "[t]he existence of a property right is but one element in determining whether expectations of privacy are legitimate." This likely comes as no surprise to an American living in the post-September 11th world, a world in which major cities like New York City have deployed thousands and thousands of cameras to cover a vast majority of the city's streets.

Many people, particularly in these densely populated urban areas that could very likely be terrorist targets, do not seem to mind all the surveillance; they simply go about their lives as usual. Those in favour of the vast system of cameras will label anyone who objects as weak on national security. What these critics fail to realize is that by accepting this level of surveillance, Americans are giving up privacy in other contexts. While the level of privacy given up may be minimal and acceptable to the masses, many would be disheartened to learn that by allowing that surveillance, they could be jeopardizing themselves in a criminal sense at a later date. That is, in a broader sense, society determines what is reasonable for the objective prong of the Katz test, and even more broadly, the Fourth Amendment.

"[T]he Katz test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations." Essentially, this hypothetical reasonable person is a reflection of society as a whole. The concern is that "[d]ramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes." Simply put, the preceding statement by Justice Alito in Jones is why cities with extensive grids of surveillance cameras are worrisome. Society grows accustomed to this level of intrusion, and it is undoubtedly an intrusion. These cameras are surely helpful in many instances. It is not the cameras themselves and their national security purpose that are troublesome. It is the expectation that they create. These cameras erode the objective expectation of privacy. Justice Sotomayor, like Justice Alito, seems sceptical as well:

> "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques."

It is legal, as has already been established, for government to employ these cameras in public areas and along public roadways. Technically speaking, government could still find out exactly where someone goes at every point, but it would require additional effort. In a way, it is like the old surveillance teams that would have to stake out a location and follow a suspect. Both provide an inherent check since they are resource intensive. It would require additional effort for law enforcement personnel to follow an individual on multiple cameras and to multiple storefronts and residences. Government could still determine who lives in which apartment building and which church or political office a person visited. The ease of access via GPS is what is so concerning.

The legislature could act to preserve the objective expectation of privacy. Justice Alito astutely noted that "concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions." There currently exists a range of legislation covering certain electronics, such as the

Wiretap Act and the Electronic Communications Privacy Act (ECPA). However, many courts have held that "cell phones, to the extent that they provide prospective, real time location information, regardless of the specificity of that location information, are tracking devices." This is so important because tracking devices are excluded from many existing pieces of legislation. That is, "a cell phone's prospective, real time location data—whether cell site or GPS—is a communication from a tracking device." This means that the GPS location data that is at issue here "is excluded from coverage under the Wiretap Act and ECPA." The Electronic Communications Privacy Act along with the Wiretap Act both set forth the legal standards to be met in order to obtain search warrants. While these bills do not run afoul the Fourth Amendment, they do make clear the requirements and provide more than just a textually minimal, though still rather practically expansive, Amendment for guidance. In essence, tracking devices in the sense of GPS enabled smartphones are still governed by case law, as opposed to statutes like these. The Wiretap Act and ECPA "[do] not prohibit the government from obtaining prospective, real time data … Rather, such information may be obtained in the same way that the government may obtain information from a tracking device: by meeting the requirements of Rule 41 [of the Federal Rules of Criminal Procedure] and the Fourth Amendment."

There is no denying that the news media will play a significant role in the objective expectation of privacy moving forward, as it currently does. It is, in fact, what the media chooses to publish that shapes our perceptions. Moreover, the news media is more likely to report a story that involves mass public outrage. Coincidentally, there has recently been public outrage regarding smartphones. In fact, the media has even taken an angle whereby it portrays the use of snooping technology on smartphones as being linked to law enforcement efforts. Forbes published online a report asking readers if they "[w]ant to know if Carrier IQ, the dialer- and location-sniffing software installed in millions of phones, is being used by the FBI for law enforcement investigations?" Forbes then followed by saying that "[t]he FBI won't reveal much about the controversial application, and why not? Because, the Bureau says, doing so might interfere with law enforcement investigations." Naturally, Americans are sceptical of private companies snooping on their phones, but nothing outrages Americans more than the government taking advantage of such techniques. While many are content with cameras spanning the country, accessing their mobile phones is completely contrary to their expectations and what they are willing to accept. Furthermore, in response to the Carrier IQ story, Senator Al Franken sent letters to the creator of Carrier IQ and to several handset manufacturers asking for additional information regarding the privacy implications.

Carrier IQ is a program that many mobile phone providers have placed on the phones they sell to consumers, and it tracks much of what a user does. The companies claim it is to assist with network improvements and that may very well be true. If Americans are so outraged by using their information for network improvements, it is unlikely that they will take lightly the government using their phones to track them with the stated purpose of potentially gathering evidence.

The Washington Post reported online that "Congress has spent much of this year debating an online privacy bill that would strengthen consumer rights when it comes to data collection — including the possibility of making it illegal in some cases to collect information without your direct consent — but it will probably still be years before the legal framework is in place. Until then, the companies that we buy our technology from need to do all they can to ensure they don't lose our trust." That same Washington Post commented that "[t]he moment they violate that trust, I won't be a Google customer anymore." It is all good and well to indicate that if a private company such as Google violates one's trust as a consumer, one will simply stop using the services of that company. However, when government violates a citizen's trust, that person cannot just stop being a customer of the United States Government, so to speak. The government is here to stay; it will not simply shut as easily as a private company. Needless to say, the government has no immediate incentive to keep citizens happy the way a private company, driven by profits, does. And, with no other immediately viable option, government knows citizens cannot simply switch services. Additionally, the government is not seeking simply to find out someone's web habits in order to send more pertinent advertising to the side of his web browser. And, on top of that, there is a much heftier price to pay when the government goes snooping. Sometimes, one may even lose his life.

4. United States v. Jones – What did the Court actually limit?

It is not often in recent history that the United States Supreme Court has delivered a unanimous decision. The justices voted nine to zero against the government's ability to install a GPS transponder on a private citizen's private vehicle without a warrant. *United States v. Jones* involved a nightclub owner suspected of being involved in the trafficking of narcotics. Federal agents applied for a search warrant to place a GPS transponder on the suspect's vehicle. Police installed the transponder in the wrong jurisdiction and after the date specified by the search warrant. Government then tracked Jones for four weeks using GPS and determined that his car, and by extension he too, visited several locations associated with narcotic trafficking. Jones was arrested, and at trial, moved to suppress the evidence obtained from the allegedly illegally placed GPS transponder.

There were two concurring opinions, one solely authored by Justice Sotomayor, who joined in the majority, and another by Justice Alito and joined by the rest. The concurring opinion in this case might as well have been a dissent as it fiercely attacked the rationale of the majority. Even Justice Sotomayor, who joined in the majority opinion, noted that "the trespassory test applied in the majority's opinion reflects an irreducible constitutional minimum: When the Government physically invades personal property to gather information, a search occurs. The reaffirmation of that principle suffices to decide this case." The crux of Justice Sotomayor's opinion is that while the Court managed to find a way to decide this case in the way that all nine justices felt the law supported, the majority simply failed to address any of the questions undoubtedly raised by the fact pattern at hand. While the Jones opinion was highly anticipated, it was not particularly helpful since the majority relied in large part on the trespassory nature of the installation of the transponder.

The Court was very clear to indicate that placing a GPS transponder on a private vehicle is a search. However, the Court failed to decide whether such a search is reasonable and does not require a warrant, or whether that search is unreasonable without a warrant and probable cause. So, the legal community now knows that placing a GPS transponder on a car is a search. All that really means is that there could be a Fourth Amendment implication. The Court acknowledged that the question of reasonableness is a necessary and proper one when it deflected it by stating that the argument was waived when the government failed to raise it in the lower court.

The concurrence stated that "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to Katz analysis." The majority attempted to head off the heavy criticism of the concurrence by stating that it was simply applying "an 18th-century guarantee against unreasonable searches, which [it] believe[s] must provide at a minimum the degree of protection it afforded when it was adopted." The majority went on to state that the concurrence "would apply exclusively Katz's reasonable-expectation-of-privacy test, even when that eliminates rights that previously existed." The point made here is that a reasonable expectation of privacy could change with society since there is both an objective and subjective element to the Katz test, both of which will be further explored in Part III. Basically, the majority wants to guard against the whims of the public and changing societal values and, thus, preserve objective expectations of privacy. The ironic part is that the majority does not carry over the rationale behind its statements since it fails to come full circle and say that placing a GPS transponder on a vehicle is an unreasonable search; it simply holds that there is a search.

The concurrence further criticized the notion that the majority was holding on to the idea that the Fourth Amendment protects places. It is well-established law that "the Fourth Amendment protects people, not places." While the Fourth Amendment undoubtedly still protects places in the sense that it still protects a person's home, the guiding principle is to protect the people by protecting their homes and effects. The home, itself, is not protected; it is the person that is protected from what could be found in his home. This same idea is applicable to a vehicle, an effect. It is not the actual vehicle itself that is protected. It is the person to whom the vehicle belongs that is protected from whatever incriminating or completely innocent evidence can be obtained by searching that vehicle. Placing a GPS transponder on that vehicle is certainly contrary to the idea of protecting the person, for it is that person's whereabouts that are the true subject of the search. And, the concurrence is correct when it states that "[i]n cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance." Not only does the majority's "reasoning largely [disregard] what is really important (the use of a GPS for the purpose of long-term

tracking)", but it "instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way with the car's operation)."

While the Court has unequivocally held that there is a search when a GPS transponder is placed on a private vehicle, it has declined to decide the reasonableness of the aforementioned search. This is largely because the government failed to raise the argument that although a search, it was a reasonable one. Presumably, if the search is found to be reasonable, it is not violative of the Fourth Amendment and there is no need for a warrant.

Fortunately, the concurring opinions in the Jones case have provided some insight. The concurring justices have alluded to the fact that the Katz reasonable expectation of privacy test would be immensely helpful in deciding future cases involving electronics. These justices find that there is no need for just an isolated initial decision as to whether a search occurred. This is particularly helpful since placing a GPS tracker on a vehicle is distinguishable from using the GPS embedded in a smartphone, which involves no physical intrusion. Accordingly, the search language from Jones does not provide a bright line rule in the realm of using built-in GPS, on either a vehicle or a smartphone.

All that can be learned from the majority opinion is that there is a search. Further, it is rather clear that the physical intrusion alone constitutes a search, and the Court states that the physical installation and monitoring constitutes a search. What remains unclear is whether the monitoring alone, as is the case with built-in GPS, is a search. The concurrence finds that the best approach "is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated."

5. Can there be an expectation of privacy when an individual voluntarily provides information to third parties?

There is no law stating that a person must have a cell phone. In fact, strictly speaking, it is not even a necessity; people do not need phones. Practically speaking, it is a much different story. Imagine that someone leaves for work or school in the morning and realizes that he left his cell phone on the kitchen counter. The vast majority of Americans would immediately turn back, assuming they were not already approaching their destination or hours down the road. The fact is, whether for safety or just habit, Americans do not often part with their cell phones. In fact, most find it so vital that mobile phone providers even sell insurance to help cover replacements. Quite simply, Americans want a new phone right away.

In a world where smartphones can now do a whole range of convenient things, like allow a user to check email on the go or surf the Internet in full form, people voluntarily share massive of amounts of information. Just because an individual "voluntarily" shares his email with a provider does not mean that he expects that the emails and their contents are not private. Justice Sotomayor points out the level of injustice individuals might feel when they learn of this when she states, "I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year." However, the law, in its current form, does not grant an expectation of privacy when information is voluntarily disclosed. Those emails are voluntarily disclosed in the sense that no one has to check email on their smartphone. In fact, no one even has to use email. It is hard to imagine not using email in a business or school today, with some companies and universities actually requiring employees and students to use email. Justice Sotomayor observed that "whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."

With the way technologies are becoming increasing integrated into our everyday lives, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." Moreover, the current "approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers."

Furthermore, medications could give clues as to a person's medical history, yet medical history is something so well protected by the law. It seems impossible that disclosing medications to a pharmacy, online or otherwise, could breach the level of confidentiality awarded to a person's medical records. Doctors do not often have to give actual medications to their patients. Pharmacies are a necessary middleman in the process. And, undoubtedly, medication is a necessity for many people. Try telling a diabetic that he does not need insulin, and that, in the broader sense of information not so narrowly tailored to cell phones or GPS, by disclosing his prescription to a pharmacy online, he sacrifices the privacy of his medical records. This area of the law considers all information that is "voluntarily" disclosed, not just information disclosed via a cell phone or just GPS data.

What is troublesome is the idea that "[n]ew technology may provide increased convenience or security at the expense of privacy, and many people may find the trade-off worthwhile," and what is actually scary is that "even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable." Justice Alito is absolutely correct here. There is, essentially, a snowball effect. What seems like a trifling erosion of privacy is simply allowed, but it then allows the next erosion to begin. It is essential to stand up each time privacy is violated in order to maintain a certain expectation. The reasonable expectation is definitely shaped by what society allows. If no one proclaims a violation as wrong, then society will just classify it as being now reasonable and thus unprotected. Take, for instance, Representative Ron Paul of Texas, who adamantly opposes both the Federal Reserve and the Transportation Security Administration ("TSA"). Although he is currently on the campaign trail seeking the 2012 republican presidential nomination, he made his way back to Washington, D.C. just to question the Chairman of the Board of Governors of the Federal Reserve System, Ben Bernanke. Likewise, Representative Paul rarely misses an opportunity to criticize the TSA for what he sees as a violation of the Fourth Amendment that is perpetrated each day at airports throughout the country. Whether Representative Paul's views are correct or not, the point is that he sets the example for standing up for privacy and for the Fourth Amendment, in relation to the TSA specifically, on a regular basis, despite the cold shoulder he often receives in response.

On another note, many Americans now use automated toll collection systems. "On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of that convenience." Motorists place a transponder in their vehicle that can be read by an overhead scanner as they pass under a pole without even having to stop or slow down. In a sense, this is a very limited GPS system. The government has control of this system and the system records each place a person's vehicle, and that person, goes on toll roads. The government could, conceivably, determine the rate of travel as well as where travel originates and where the driver exits the toll system. Individuals voluntarily enrol in this system. There is still the option to pay with cash in most places. However, even using cash, clearly visible cameras capture every license plate in an effort to fine those who fail to pay. Government can track individuals on these toll roads.

This automated toll collection system is a bit different than placing cameras on roads since it pinpoints where a person is without any further research; there is no need to run a license plate through the database. The key difference is that individuals voluntarily place this transponder in their vehicle. When an individual voluntarily places the transponder in his car, he knows that the government runs the program. This makes it easily distinguishable from mobile phones. Most service providers are publicly traded companies. The government does not run them. The transponder is used for the very narrow purpose of paying tolls and individuals are aware by logging into an account online that the government tracks each scan. The expectation of privacy is different in the case of automated toll collection systems. The transponder is voluntarily placed in the person's car with knowledge of a government connection.

Smartphones are not thought of as having a government connection. There is no existing agreement with the government for the use of the smartphone, except perhaps to pay government taxes as a part of the mobile service bill. Additionally, there is almost never an expectation of privacy in one's location on and along public roadways

Similarly, "[m]any motorists purchase cars that are equipped with devices that permit a central station to ascertain the car's location at any time so that roadside assistance may be provided if needed and the car may be found if it is stolen." This program, unlike the automated toll collection, is with a private company. It is for an extremely limited purpose. Further, it is unlike a cell phone in that people expect that cell phones are constantly emitting signals. Individuals only expect this system in a car to be activated when the car is reported as stolen or the driver calls for assistance. Given the limited scope and the private nature of this service, government would have a steep mountain to climb to show that there is

a voluntary disclosure here. In fact, the driver does not voluntarily disclose GPS data to the company on a regular basis like with a smartphone. The driver hopes, in purchasing this on-board system, to never have to use it.

There is another phenomenon that has invaded the homes and mobile devices of many Americans these days, social networking. Facebook and Twitter are two of the most popular. It is now typical to find that "phone-location-tracking services are offered as 'social' tools, allowing consumers to find (or to avoid) others who enrol in these services." Two such services are the Facebook check-in and Foursquare. Both of these programs run through the social networking interface and allow users to notate when they and friends are at particular locations. Sharing this type of information is voluntary. In fact, users on Facebook can disable the ability of others to check them in at locations. More substantially, broadcasting one's location on social media sites shows no expectation of privacy. One can set his Facebook to be viewed by friends only, and therefore, the information is not available to the general public. However, most individuals have hundreds of "friends" meaning that while the content is not available to every user, it is still voluntarily shared with a large number of third parties. Providing information on social networks regarding your GPS location via your smartphone shows absolutely no subjective intent to keep your location private. Government could very likely use this type of GPS data without a warrant and with little difficulty under a Katz analysis. Users are aware that Facebook is a means to communicate with third parties. Facebook users are unlikely to expect privacy in the GPS data that they freely upload for others to see, and society is unlikely to find an expectation of privacy in self-published GPS data to be reasonable. It is unlikely that this technique would be seen as a search under the Fourth Amendment.

Despite the acknowledgement by Justice Sotomayor that a change may be needed, if information is voluntarily disclosed, then there can be no expectation of privacy. Apple's iPhone has become extremely popular, with consumers camping out overnight to purchase the next model. Many smartphone users have iPhones. The iPhone, in particular, has an option to turn off what it calls "Location Services." This setting controls access to the built-in GPS for individual applications or for the phone as a whole. By turning off all location services (all GPS functionality), a user is undeniably showing a subjective expectation of privacy in his location. There is a strong argument that society would be willing to find that as reasonable since the user has taken an articulable action to demonstrate a desire for privacy.

For argument's sake, assume that society finds an expectation of privacy to be reasonable after turning Location Services off. Thus, there is now a setting whereby an individual can reasonably expect privacy in the GPS data from the transponder built into his smartphone. What if GPS data is still broadcast even when a user turns all location services off? Just this past year, it was reported that "Apple Inc.'s iPhone [was] collecting and storing location information even when location services [were] turned off, according to a test conducted by The Wall Street Journal." Users became outraged and "Apple Inc. (AAPL) was sued for alleged privacy invasion and computer fraud by two customers who claim the company is secretly recording and storing the location and movement of iPhone and iPad users." It would seem that the issue to be decided is whether a user expects by purchasing a smartphone with built-in GPS that there is no expectation that the GPS data can ever be stopped. Given what was recently learned about the iPhone, it seems as though there is really no way to control what the smartphone does behind the scenes, despite user commands. The smartphone may still continue to collect GPS location data. A user may not have a choice even after making a conscious decision to stop voluntarily providing GPS information to third parties.

From a practical standpoint, the use of the location data from smartphones may not be all that government would hope it to be. Burner phones, or prepaid phones, throw a huge wrench into the ability to track criminals. Many criminal enterprises make use of these burner phones, which are relatively cheap prepaid phones that can be discarded with relative ease. If the reason for using smartphone location data is to gather evidence to charge suspected criminals, then the idea that criminals change phones often would make determining what phone is being used nearly impossible. The larger implication is that all location data could be stored and then government given the opportunity to figure out which phones belong to whom later.

Suspected criminals are less likely to switch vehicles as readily as phones. However, study after study has shown that crime is most prevalent in densely populated urban areas. It is those same urban areas where individuals tend to rely on public transportation. The reliance on public transportation in cities cuts across every socio-economic background. Many middle class individuals that could afford cars simply do not bother because of traffic and opt instead for buses or subways. As it turns out, phone-tracking could be the best option if these suspected criminals do not use vehicles in urban settings.

Vehicle GPS tracking certainly has its limited place, when done in accordance with the law, but the danger of smartphone GPS tracking is far more expansive and spans every socio-economic position.

6. Conclusion

It is conceivable that a mobile service provider stores the location data derived from GPS transmissions from the smartphones of its users. This information could be maintained and stored for lengthy periods of time. When corporations are convicted criminally, it usually results in large financial penalties. There is certainly the possibility that corporations could trade GPS location data on users in exchange for leniency from the government in a pending legal matter. If users voluntarily share this location information, only a contractual relationship could provide for its confidentiality. Current user agreements may be written so broadly that providers might possibly even have the ability to make an argument for sharing location data already.

Laws are great protection; however, sometimes the damage is already done. "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." Neither monetary damages nor an injunction are going to take back from the government's knowledge or, even more so, the public domain knowledge about a person's whereabouts. More specifically, "[d]isclosed in [GPS] data ... [could] be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." The release of this location data could show that a woman visited an abortion clinic. The law cannot undo the release of that extremely private information; perhaps her parents now disown her or something of the sort. The biggest fear in a country based on liberty is that the "[a]wareness that the Government may be watching chills associational and expressive freedoms."

Government's desire to track citizens using the GPS data from their smartphones "implicate[s] the questions of whether and under what circumstances continuous GPS surveillance constitutes a 'search' under the Fourth Amendment, thereby necessitating probable cause and a warrant." The Court answered in Jones by indicating that it "need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4–week mark." Tracking the GPS of a smartphone would likely become a search after four weeks. After just a day though, it could follow that there is no search. If the Court drew the mark at a definite search being that four-week period, then it would seem as though there must be a point when there is no search. Maybe a day is even too generous. The Court seems to conclude that the length of the monitoring is a significant factor in determining if a search has occurred. What is clear though is that "where uncertainty exists with respect to whether a certain period of GPS surveillance is long enough to constitute a Fourth Amendment search, the police may always seek a warrant."

As for the individual, it appears as though the GPS data is voluntarily shared with a third party, the service provider. Accordingly, that information is not afforded an expectation of privacy and would fail the Katz test, making it ineligible for Fourth Amendment protection. Unless and until the legislature acts or the Court decides to change the presumption that currently flows from voluntarily sharing information with a third party, the tracking of the built-in GPS of smartphones is not afforded protection. The Court could, however, find that individuals subjectively demonstrate an expectation of privacy in that location data sent from their smartphones and that society is willing to accept that expectation as reasonable. This could allow the Court to find that the voluntarily disclosure is one that society finds to have a reasonable expectation of privacy when communicated from a smartphone for the sole purpose of providing services that a user has paid for

.* * * * *

Cite as: Heidel, Eric Samuel. Warrantless GPS Tracking: Who cares about vehicle transponders – what about your cell phone? .*Journal of International Commercial Law and Technology*, Vol.8 No.1 (January, 2013)