January 17, 2014

Checked In: Real-time Geolocation Surveillance and the Fourth Amendment

Eric J Struening, American University Washington College of Law

Available at: https://works.bepress.com/eric_struening/1/
Eric J. Struening
Checked In: Real-time Geolocation Surveillance and the Fourth Amendment
The Fourth Amendment is perhaps the most powerful protection an individual has against the Government invading their lives. The framers adopted this amendment because of their experience with British general warrants prior to the Revolution.¹ Those general warrants provided British authorities “license to ‘break into any shop or place suspected’ where ever and whenever they chose. With that kind of unfettered discretion, the general warrant could be, and often was, used to intimidate.”² The Fourth Amendment specifically prevents this type of intrusion by the Government. It provides: “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated, and no Warrants shall issue, but upon probable cause . . . .”³ However, there has always been an open question of how far the protection of the Fourth Amendment provides an individual against Government intrusion, especially when new technology is used.

There are two theories to Fourth Amendment protection, the property theory⁴ and the privacy theory.⁵ Under both theories, if a person has a reasonable expectation in their property or in their privacy then the Government must obtain a warrant, prior to its search.⁶

While a warrantless search is “per se unreasonable,”⁷ there are numerous exceptions that allow warrantless searches to be performed without violating the Fourth Amendment. These include: searches incidental to a valid arrest,⁸ “stop and frisk” searches,⁹ “hot pursuit” or exigent

---

³ U.S. CONST. amend. IV.
⁶ See Jones, 132 S. Ct. at 949; Katz, 389 U.S. at 347.
⁷ Katz, 389 U.S. at 357.
circumstances searches,\textsuperscript{10} the use of pen registers,\textsuperscript{11} the contents of banking records,\textsuperscript{12} searches to prevent railroad accidents that cause “great human loss,”\textsuperscript{13} searches of persons and things entering and leaving the United States,\textsuperscript{14} and searches of boats on navigable waters.\textsuperscript{15} This paper seeks to determine if the Government is required to obtain a warrant in order to obtain a person’s geolocation data for national security purposes.

The answer to if a warrant is required has a great impact in both realms of criminal investigations and national security. Many of the same techniques are used to gain information about threats to national security and in investigating crimes.\textsuperscript{16} These techniques include wiretaps, undercover agents, physical searches, and “more recently, sophisticated computer technologies, including e-mail intercepts and data mining.”\textsuperscript{17} Geolocation is another one of these techniques.

Geolocation provides the user with data that reveals a piece of technology’s geographic location, and with it, the location of the person using that technology.\textsuperscript{18} This information can be provided by technology such as, but not limited to, location beepers, Global Positioning System (GPS) devices, and cellular phones.\textsuperscript{19} Currently, there are three main techniques used to generate

\begin{footnotesize}

\textsuperscript{11} Smith v. Maryland, 442 U.S. 735 (1979).
\textsuperscript{14} United States v. Montoya de Hernandez (473 U.S. 531 (1985).
\textsuperscript{16} STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 553 (5th ed. 2011).
\textsuperscript{17} Id.
\textsuperscript{18} In the Matter of the Application of the United States for an Order Authorizing the Monitoring of Geolocation and Cell Site Data for a Sprint Spectrum Cell Phone Number ESN, 2006 WL 6217584 (D.D.C 2006).
\end{footnotesize}
this type of information: the collection of cell-site data,\textsuperscript{20} GPS data,\textsuperscript{21} and wireless geolocation.\textsuperscript{22} Some emerging geolocation technologies, such as Bluetooth beacons, “have the potential to pinpoint the location of a phone to a matter of inches.”\textsuperscript{23}

This paper will discuss how the Fourth Amendment applies to real-time geolocation tracking for national security purposes. I will begin by discussing the different legal regimes of Fourth Amendment searches Title III (domestic or criminal purposes) and FISA (foreign intelligence purposes) and when, under those regimes, a warrant is required for surveillance. Then because “the Court must first look to whether the [surveillance] falls within the ambit of [the Fourth Amendment] at all” before deciding if a warrant is required,\textsuperscript{24} I will discuss the application of the Fourth Amendment to geolocation surveillance through briefly discussing the property theory of the Fourth Amendment, and then focusing on the privacy theory of the Fourth Amendment through applying the \textit{Katz} test. To apply the \textit{Katz} test, I will first discuss what society accepts as reasonable through discussing the Court’s application of the Fourth Amendment to surveillance cases. Finally, I will discuss how the rise of technology affects how people view their expectation of privacy subjectively, and the type of information that can already be determined by using only geolocation data created by such technology.

\begin{itemize}
  \item \textsuperscript{20} “[T]he identification of the radio cell tower or towers nearest to the device” which is the oldest and least precise of the current methods. \textit{Id.}
  \item \textsuperscript{21} Radio signals are received by the device “from a system of satellites in geosynchronous orbit and interpreted by programs to provide highly accurate location data.” \textit{Id.}
  \item \textsuperscript{22} Operates by comparing the access points used by the [device] to connect to the Internet against a database of known router locations. \textit{Id.}
  \item \textsuperscript{23} \textit{Id.}
  \item \textsuperscript{24} Renee McDonald Hutchins, \textit{Tied Up in Knotts? GPS Technology and the Fourth Amendment}, 55 UCLA L. Rev. 409, 422 (2007) (citing to WILLIAM W. GREENHALGH, \textsc{The Fourth Amendment Handbook; A Chronological Survey of Supreme Court Decisions} 1 (2d ed. 2003)).
\end{itemize}
Surveillance Legal Regimes

First off, it must be noted that the most important determination of how the Fourth Amendment applies to real-time geolocation surveillance is whether the target is an American citizen or on U.S. soil because this determines whether the Constitution is at all applicable to the surveillance. The seminal case *Katz v. United States* established that the Fourth Amendment protects people, not places,” and that the Fourth Amendment applies to electronic surveillance as it does with physical searches.\(^{25}\) As such, when the Constitution is implicated, the surveillance must be reasonable.\(^{26}\) However, the Fourth Amendment only protects the people of the United States against actions by their own government, and does not extend the same protection to non-Americans outside the boundaries of United States territories.\(^{27}\) Therefore, the Fourth Amendment is not implicated in surveillance against foreign persons on foreign soil, and such surveillance is not required to be reasonable.\(^{28}\)

The second determination about the target is the purpose of the surveillance. The reason why the Government seeks out a person’s geolocation data will dictate what procedures the Government must follow to receive a warrant or judicial approval in order to obtain that data. Without obtaining such approval, the surveillance would be likely to be found unreasonable.\(^{29}\) If the surveillance is performed for criminal investigations purposes, including domestic security,


\(^{26}\) Id.

\(^{27}\) United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990) (“The available historical data show, therefore, that the purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own Government; it was never suggested that the provision was intended to restrain the actions of the Federal Government against aliens outside of the United States territory.”).

\(^{28}\) See id.

\(^{29}\) See *Katz*, 389 U.S. at 357 (“. . . that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment subject only to a few specifically established and well-delineated exceptions”).
the surveillance is governed by one rule, and if the surveillance is performed for foreign intelligence purposes it is governed by another rule. Each of these rules requires a different type of probable cause to obtain the warrant.

1. Domestic Surveillance

The Supreme Court in *Katz* held electronic surveillance that is performed with the purpose of investigating a crime falls under the warrant provision of the Fourth Amendment. However, the Court specifically declined to answer whether a warrant would be required “in a situation involving the national security.” To address *Katz*, Congress established a procedure for court authorization of electronic surveillance used to investigate specific crimes under Title III of the Omnibus Crime Control and Safe Streets Act, but this too did not explicitly address national security. To obtain a Title III warrant for surveillance the Government must show:

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated [in Title III];
(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;
(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;
(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

---

32 389 U.S. at 347.
33 Id. at 358 n.23.
The Supreme Court then addressed the warrant requirement for domestic national security matters in *United States v. United States District Court (Keith).*\(^{36}\)

In *Keith*, the Court answered the question left open by *Katz*: “whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security. . ..”\(^{37}\) The Government performed a wiretap with the purpose of obtaining information about a domestic terrorism plot that was authorized only by the Attorney General and not a court.\(^{38}\) “[T]he Government asserted that the surveillance was lawful, though conducted without prior judicial approval, as a reasonable exercise of the President’s Power (exercised through the Attorney General) to protect the national security.”\(^{39}\) The Court rejected this assertion, finding instead that “these Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch.”\(^{40}\) The Court therefore held “that prior judicial approval is required for the type of domestic security surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.”\(^{41}\) Congress later amended Title III to include electronic surveillance for numerous domestic national security reasons.\(^{42}\)


\(^{37}\) *Id.* at 309.

\(^{38}\) *Id.* at 297.

\(^{39}\) *Id.* at 301.

\(^{40}\) *Id.* at 316-17.

\(^{41}\) *Id.* at 324.

2. Foreign Intelligence Surveillance

While the Court in Keith addressed domestic surveillance on national security, it specifically declined to address if a warrant was required for electronic surveillance for foreign intelligence purposes.\footnote{43 407 U.S. at 321-22 (“We have not addressed and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents.”).} Title III is also silent on foreign intelligence surveillance.\footnote{44 \textit{See generally} 18 U.S.C. §§2510-2520.} Where electronic surveillance\footnote{45 Electronic surveillance is defined at 50 U.S.C. §1801 (f).} is conducted inside the United States or against a U.S. person with a significant purpose of obtaining foreign intelligence information\footnote{46 Foreign intelligence information is defined as “(1) information that relates to, and if concerning a United States person is necessary to the ability of the United States to protect against – (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to – (A) the national defense or security of the United States; or (B) the conduct of the foreign affairs of the United States.” 50 U.S.C. §1801 (e).} between “foreign powers” and “agents of foreign powers” the Foreign Intelligence Surveillance Act (FISA) applies.\footnote{47 50 U.S.C. §§1801-1881g (2006 & Supp. III 2009), as amendment by Pub. L. No. 111-259, §801, 124 Stat. 2654, 2746 (2010) (see also \textit{In re: Sealed Case Nos. 02-001, 02-002}, Foreign Intelligence Surveillance Court of Review, 310 F.3d 717 (2002) (discussing the USA Patriot Act amendment changing FISA’s application from primary purpose to significant purpose).} Like the Fourth Amendment itself, FISA does not apply outside the United States to non-U.S. persons, only to foreign powers and agents of foreign powers. FISA defines both “foreign powers” and agents of “foreign powers. Foreign powers under FISA include: foreign governments, factions of foreign nations, international terrorist groups, foreign based political organizations or an entity that is engaged in the proliferation of weapons of mass destructions, all of which are not substantially composed of United States persons.\footnote{48 50 U.S.C. §1801(a).} Agents of a foreign power include someone other than a United States person who: acts as an officer or employee of a foreign power, acts on
behalf of or is directed by a foreign power that engages in spying against the United States, engages in or assists in the preparation of international terrorism.\textsuperscript{49} The statute also defines United States person as:

\begin{quote}
 a citizen of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power. \ldots \textsuperscript{50}
\end{quote}

FISA is Congress’s “attempt to fashion a ‘secure framework by which the Executive Branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation’s commitment to privacy and individual rights.’”\textsuperscript{51} As part of this framework, FISA created the Foreign Intelligence Surveillance Court (FISC), a special court to oversee such surveillance, which is closed from the public due to the sensitive nature of foreign intelligence.\textsuperscript{52} The FISC can issue a warrant for electronic surveillance if the judge finds that based on the facts submitted in an application by a Federal official and approval by the Attorney General, there is probable cause to believe that “the target of the electronic surveillance is a foreign power or an agent of a foreign power;”\textsuperscript{53} “each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power,” minimization procedures will be followed, and that the application includes a statement certifying that “the information sought is the type of foreign information

\begin{itemize}
  \item \textsuperscript{49} *Id.* at §1801(b).
  \item \textsuperscript{50} *Id.* at §1801(i).
  \item \textsuperscript{52} 50 U.S.C. §1803.
  \item \textsuperscript{53} A United States person cannot be designated a foreign power or an agent of a foreign power based solely on First Amendment protected activity. §1804 (a)(2)(A).
\end{itemize}
designated; and such information cannot be obtained by normal investigative techniques.\textsuperscript{54} While the same probable cause is not required for obtaining a FISA warrant as is required for obtaining a Title III warrant, it is reasonable under the Fourth Amendment nonetheless.\textsuperscript{55,56}

**Property Protection of the Fourth Amendment against surveillance**

The Fourth Amendment protects against a physical trespass by the Government on to a person’s property, even with the purpose of obtaining information.\textsuperscript{57} Therefore, it matters how the Government gets the geolocation tracking device into the hands of the target. As the majority in *United States v. Jones* recognized, when a tracking device is physically installed on a person’s private property, it is a search under the Fourth Amendment requiring a warrant.\textsuperscript{58} However, when a tracking device is physically installed on something (i.e. a car, a container, or a cell phone) prior to the target of the surveillance taking possession of that item, the person’s Fourth Amendment rights are not violated by the installation.\textsuperscript{59} The installation of a tracking device only signifies the potential for an invasion of privacy, and the Court has “never held that potential, as

\textsuperscript{54} 50 U.S.C. §1804(a).

\textsuperscript{55} In re Sealed Case, 310 F.3d 717, 746 (Foreign Int. Surv. Ct. Rev. 2002) (“[W]e think the procedures and government showing required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close. We, therefore, believe firmly, applying the balancing test drawn from Keith, that FISA as amendment is constitutional because the surveillance it authorizes are reasonable.”)

\textsuperscript{56} FISA also provides for warrantless surveillance in two cases- In an emergency situation for up to 72 hours, after which the surveillance must be approved by the FISC or ended, and for a systematic surveillance of communications between two foreign powers where “there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and” the surveillance follows minimization procedures. 50 U.S.C. §1805(f); 50 U.S.C. §1802 (a)(1). 50 U.S.C. §1802 (a)(1).

\textsuperscript{57} *United States v. Jones*, 132 S. Ct. 945, 949 (2012) (finding that the physical installation of a tracking device on Jones’s property was a Fourth Amendment search because it is a physical intrusion on his property by the government).

\textsuperscript{58} *Jones*, 132 S. Ct. at 949.

opposed to actual, invasions of privacy constitute a search for purposes of the Fourth Amendment.\textsuperscript{60} This also extends to tracking devices already present and not installed by the Government, such as GPS technology on a cellular phone.\textsuperscript{61}

**Privacy Protection of the Fourth Amendment**

In addition to property interest protection in the Fourth Amendment, the Supreme Court added in *Katz v. United States* that there was also a privacy interest in the Amendment, and that a physical intrusion onto someone’s property is not required for a Fourth Amendment violation.\textsuperscript{62} *Katz* found that “what a person knowingly exposes to the public, even in his own home or office is not subject to Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public may be constitutionally protected.”\textsuperscript{63} The Supreme Court concluded that the Government had violated Katz’s reasonable expectation of privacy when his conversation was heard by the Government through electronically eavesdropping.\textsuperscript{64}

While Justice Stewart wrote the majority decision in *Katz*, the lasting impact of the case comes from Justice Harlan’s concurrence where he developed a two-pronged test for determining if a search has occurred under the Fourth Amendment.\textsuperscript{65} Harlan wrote “that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and,

\begin{itemize}
\item \textsuperscript{60} *Id.* at 781.
\item United States v. Skinner, 690 F.3d 772, 781 (6th Cir. 2012) (finding the defendant could not object to the presence of GPS on his cell phone because the government never had physical contact with it and the GPS technology was already present when he obtained the phone).
\item 389 U.S. 347 (1967).
\item *Id.* at 351-52.
\item *Id.* at 355.
\item *Id.* at 361 (Harlan, J., concurring).
\end{itemize}
second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”  

From this test he concluded

... a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the ‘plain view’ of outsiders are not ‘protected’ because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.

While only a concurrence, Harlan’s test has been adopted by the Supreme Court in multiple cases as the “lodestar” for determining if a search has occurred. Therefore, in looking at real-time geolocation tracking to determine if the Fourth Amendment is implicated, it must be determined what a person can subjectively expect to keep private, and what the public has deemed to be reasonable. While Justice Harlan’s Katz test puts the subjective component as the first prong, for a global analysis of real-time geolocation tracking, it is more effective to first determine what society has already accepted as a reasonable expectation of privacy against electronic surveillance.

1. Expectation of privacy against geolocation tracking society has accepted as reasonable

In looking at what society has recognized as having an expectation of privacy, guidance can be taken from where courts have already found such an expectation to exist. From these cases, there are three separate components that influence determining if society views the Government’s real-time geolocation surveillance as reasonable; the technology used by the

---

66 Id.
67 Id.
government to track the target, the time spent tracking the target, and if the data is created by third party surveillance.

A. Technology Used

In judging the reasonableness of a privacy expectation against an electronic search, the Supreme Court has relied on the type of information the technology reveals during the surveillance. The type of information falls into two distinct groups: sense-augmenting surveillance and extrasensory surveillance.69 “Sense-augmenting surveillance refers to surveillance that reveals information that could theoretically be attained by one of the five human senses.”70 Extrasensory surveillance is surveillance that “reveals information otherwise indiscernible to the unaided human senses.”71 The Court has generally allowed sense-augmenting surveillance as reasonable, while finding that extrasensory surveillance requires a warrant.72

i. Sense-augmenting surveillance

“Nothing in the Fourth Amendment prohibit[s] the [Government] from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology” allows.73 This principle dates back to 1927 when in United States v. Lee the Supreme Court found that the use of a searchlight to aid in looking into dark areas below a ship’s

69 Hutchins, 55 UCLA L. Rev. at 432.
70 Id. at 432-33.
71 Id. at 433.
72 Id.
deck did not require a warrant.\textsuperscript{74} The Fourth Amendment is also not implicated when technology can also be used to change a person’s viewpoint.\textsuperscript{75}

In addition to aiding the senses, it does not become a search when technology is used to augment the senses, even when the person would not be there to sense them. In \textit{United States v. Knotts}, the Court considered if law enforcement’s tracking of a target on public roads to a cabin by following a beeper placed into a barrel, which was then sold to the target constituted a Fourth Amendment search.\textsuperscript{76} “A beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver.”\textsuperscript{77} Typically beepers only enable the tracker to determine if the device is nearby.\textsuperscript{78} The Court used the \textit{Katz} analysis to determine that the use of the beeper was not a Fourth Amendment search, because it was akin to visually following his car on public streets and highways.\textsuperscript{79} “

A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the defendant] travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.\textsuperscript{80}

However, this augmentation is limited to what the Government can have the capability to sense. In \textit{United States v. Karo}, law enforcement also used a beeper to track a suspect, however,

\begin{itemize}
  \item \textsuperscript{74} 273 U.S. 559, 563 (1927) ("Such use of a searchlight is comparable to the use of a marine glass or a field glass. It is not prohibited by the Constitution.").
  \item \textsuperscript{75} California v. Ciraolo, 476 U.S. 207, 215 (1986) ("In an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet.").
  \item \textsuperscript{76} 460 U.S. 276 (1983)
  \item \textsuperscript{77} \textit{Id.} at 277.
  \item \textsuperscript{78} Hutchins, 55 UCLA L. REV. at 435.
  \item \textsuperscript{79} \textit{Knotts}, 460 U.S. at 281.
  \item \textsuperscript{80} \textit{Id.} at 281-82.
\end{itemize}
unlike *Knotts*, law enforcement installed the beeper on to a can already possessed by the suspect and the suspect was tracked within his own home.\(^81\) The Court found that tracking the device within the home was an unreasonable search because “the Government surreptitiously employ[ed] an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house.”\(^82\) The Court also distinguished if from *Knotts* because “the information obtained in *Knotts* was ‘voluntarily conveyed to anyone who wanted to look ...,’ here, [ ] the monitoring indicated that the beeper was inside the house, a fact that could not have been visually verified.”\(^83\) Therefore, in order for sense augmenting technology to not infringe on the Fourth Amendment, it must obtain the same information that could have actually been obtained.

ii. Extrasensory Surveillance

In contrast to sense augmenting technology, the Supreme Court has been more restrictive on extrasensory surveillance. This is treatment is most evident in *Kyllo v. United States*.\(^84\) In *Kyllo*, the U.S. Department of the Interior suspected Kyllo of growing marijuana inside his home.\(^85\) To investigate this, an agent sitting outside, scanned the exterior of the home with a thermal-imaging device that was not readily available to the public.\(^86\) This scan revealed infrared radiation, which is not detectible by the human eye,\(^87\) emitting from parts of his home, revealing

\(^{81}\) 468 U.S. 705 (1984) (see also note 57 for discussion of physical installation).

\(^{82}\) *Id* at 715.

\(^{83}\) *Id.* (quoting *Knotts*, 460 U.S. at 281).

\(^{84}\) 533 U.S. 27 (2001).

\(^{85}\) *Id* at 30.

\(^{86}\) *Id.*

\(^{87}\) *Id.* at 29 (“Thermal imagers detect infrared radiation, which virtually all objects emit but is not visible to the naked eye.”).
where he grew marijuana.\textsuperscript{88} The Court found that thermal imaging was a search that required a warrant, because “obtaining by sense-enhancing technology any information regarding the home's interior that could not otherwise have been obtained without physical ‘intrusion into a constitutionally protected area,’” constitutes a search—at least where (as here) the technology in question is not in general public use.\textsuperscript{89}

Real-time geolocation tracking is a sense-augmenting surveillance technique rather than extrasensory because the same information, where the person is, can be derived from a purely visual search.\textsuperscript{90} The information obtained is identical to that gained by the beeper in \textit{Knotts}, only more exact.\textsuperscript{91} This advancement in technology should not be enough to distinguish the new technology from that of a beeper because “law enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system.”\textsuperscript{92} Further, the target does not have a legitimate expectation of privacy because the geolocation data would just be a proxy for a visual observable location, as there is “no legitimate expectation of privacy in his movements along public highways.”\textsuperscript{93} This also extends to identifying if the target is in their home as well.\textsuperscript{94} However, if the technology is used with the purpose of identifying where in a home the target is, then the tracking would be a search.\textsuperscript{95}

\textsuperscript{88} \textit{Id.}
\textsuperscript{89} \textit{Id.} at 28 (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).
\textsuperscript{90} \textit{See} United States v. Skinner, 690 F.3d 772, 778 (6th Cir. 2012).
\textsuperscript{91} \textit{Knotts}, 460 U.S. at 281.
\textsuperscript{92} \textit{Skinner}, 690 F.3d at 778.
\textsuperscript{93} \textit{Id.} at 779 (quoting \textit{Knotts}, 460 U.S. at 285).
\textsuperscript{94} \textit{Knotts}, 460 U.S. at 281-82.
\textsuperscript{95} \textit{See Karo}, 468 U.S. at 705.
B. Time spent tracking the target

In addition to the technology used, there is a growing suggestion that the length of time the Government tracks a target can implicate the Fourth Amendment, in that at some point during the time period of surveillance, one moment warrantless surveillance is reasonable and the next it is not. This concept of violating a person’s right to privacy is connected to the public/private property surveillance dichotomy. A person has the highest level of expectation of privacy while in their own home, and the Supreme Court has held that Government cannot trace a person within their home or on private property where they have an expectation of privacy. However, the Supreme Court also found that a person has no reasonable expectation of privacy when their movements are traced while on a public roadway because the same information is gathered as it would if gathered visually. This includes the capability of the Government to trace someone to their home, if that information would be visually available to them.

---

96 Silverman v. United States, 365 U.S. 505, 511 (1961) (“At the very core [the Fourth Amendment] stands the right if a man to retreat into his home and there to be free from unreasonable governmental intrusion.”).
98 460 U.S. 276, 281 (1983) (“A person traveling in an automobile on a public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”); United States v. Skinner, 690 F.3d 772, 779 (6th Cir. 2012) (“we determine whether a defendant’s reasonable expectation of privacy has been violated by looking at while the defendant is disclosing to the public, and not what is known to the police.”).
99 Knotts, 460 U.S. at 281 (holding that the government could use a location beeper to track someone to their home because the person had no expectation of privacy in arriving home off of a public highway, the police could have obtained the same information visually); United States v. Dooley, 2013 L 2548969 (N.D. Ga June 10, 2013) (finding, pre-Jones, that a GPS transmitter could be installed on a person’s non-covered driveway because it was visible to the public and the person did not have an expectation of privacy.).
The idea that length of a search can implement the Fourth Amendment by violating a person’s expectation of privacy is relatively new, being first described by the D.C. Circuit in United States v. Maynard, and discussed again by the concurrences in the Supreme Court’s review of the same case, retitled United States v. Jones. The majority of the circuit court in Maynard and the concurrences in Jones each suggest that the length of time surveillance tracks a person can violate a person’s reasonable expectation of privacy.

The basic facts of Maynard/Jones are as follows: Antoine Jones was suspected of trafficking narcotics and the target of a joint FBI and Washington, DC Metropolitan Police Department task force. Based on information already gathered the Government applied to the United States District Court for the District of Columbia for a warrant to use an electronic tracking device on a Jeep registered to Jones’s wife. “A warrant [was] issued, authorizing installation of the device in the District of Columbia within 10 days,” but, the device was installed on the 11th day, not in the District of Columbia but in Maryland. Over the next 28 days, the joint task force used the device to track the Jeep’s movements. The device established the vehicle’s location within 50 to 100 feet, and relayed more than 2,000 pages of

---

103 Id at 948.
104 Id.
105 Id.
106 Id.
107 Id.
data over the period of surveillance.\textsuperscript{108} The Government used this information to obtain a multiple-count indictment against Jones.\textsuperscript{109} Before trial, Jones sought to suppress the evidence obtained through the GPS device, but the District Court only suppressed “the data obtained while the vehicle was parked in the garage adjoining Jones’s residence.”\textsuperscript{110} Jones was later convicted.\textsuperscript{111}

The D.C. Circuit reversed the conviction, focusing on the how the length of the surveillance could allow the Government to see a “mosaic” of the target’s life.\textsuperscript{112} The circuit court found:

Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.\textsuperscript{*} A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.\textsuperscript{113}

Further, the court found that “the whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil,” and therefore the surveillance was unreasonable.\textsuperscript{114}

\textsuperscript{108} Id.
\textsuperscript{109} Id.
\textsuperscript{110} Id.
\textsuperscript{111} Id.
\textsuperscript{112} Maynard, 615 F.3d at 652.
\textsuperscript{113} Id.
\textsuperscript{114} Id at 640.
On appeal, the Supreme Court unanimously agreed that the surveillance violated the Fourth Amendment and that the D.C Circuit decision should be upheld, however the Justices split on the reasons why there was a Fourth Amendment violation.\footnote{Jones, 132 S. Ct. 945; see discussion note 57.} While the majority decision written by Justice Scalia decided the case using the property-centric analysis,\footnote{Id at 949-50. (Justice Scalia focused on the Government’s installation of the GPS device onto the car. “It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a “search” within the meaning of the Fourth Amendment when it was adopted.”); see discussion supra} the two concurrences suggest that the length of time of the surveillance can implicate the Fourth Amendment.\footnote{See Fabio Arcila, Jr., GPS Tracking Out of Fourth Amendment Dead Ends: United States v. Jones and the Katz Conundrum, 91 N.C. L. REV. 1, 17 (2012) (“The ruling is considerably more complex than an ordinary 5-4 decision because, through Justice Sotomayor provided the crucial fifth vote for Justice Scalia’s opinion, she wrote her own separate concurrence in which she indicated a great deal of approval for Justice Alito’s competing approach, and a remarkable willingness to be even more aggressive applying it.”).} The fact that in the two concurrences five justices found the length of the surveillance violated Jones’s privacy preserves the idea that length of time is a factor in the reasonableness of geolocation surveillance.\footnote{Id.}

Alito’s Concurrence

Justice Alito’s concurrence, signed on to by Justice Ginsburg, Justice Breyer, and Justice Kagan, focused on how the Government violated Jones’s expectation of privacy, and relied on the decision in \textit{Knotts}.\footnote{Jones, at 958 (Alito, J. concurring) (“I would analyze the question presented in this case by asking whether respondent’s reasonable expectation of privacy were violated by the long-term monitoring of the movements of the vehicle he drove.”)} For Alito,

“the use of longer term GPS monitoring in investigations of most offenses impinges on expectation of privacy. For such offenses, society’s expectation has been that law enforcement agents and others would not – and indeed, in the main,
simply could not – secretly monitor and catalogue every single movement of an individual’s car for a very long period.”

However, Alito also found that “relatively short-term monitoring of a person’s movements on public streets accords with expectations of privacy that our society has recognized as reasonable.” While he does not describe the point in time “the tracking of this vehicle became a search,” he did find “that the line was surely crossed before the 4-week mark.” He also offered a suggestion to law enforcement because of the difficult question in finding that line, “[b]ut 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.”

Sotomayor’s Concurrence

Justice Sotomayor joined Justice Scalia’s majority, but wrote separately and wrote that she agreed with Justice Alito’s assertions about the violation of privacy expectation in GPS surveillance. She agreed with Justice Alito “that, at the very least, ‘longer term GPS monitoring in investigation of most offenses impinges on expectations of privacy,’” but was overall troubled with the idea of geolocation surveillance. Because of this concern, she also

---

120 Id at 964.
122 Id.
123 Id.
124 Id at 955 (Sotomayor, J. concurring).
125 Id. (quoting Alito, J. concurring at 964).
126 Id at 956 (“The net result is that GPS monitoring – by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track –may ‘alter the relationship between citizen and government in a way that is inimical to democratic society.’”) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (C.A.7 2011).
indicated a willingness that she would go further and find that short term monitoring could also implicated the Fourth Amendment.\footnote{127}{Id at 955. (“In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the \textit{Katz} analysis will require particular attention. 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.”).}

Alito and Sotomayor’s concurrences, when taken together, “appear[] as though a five justice majority is willing to accept the principle that government surveillance over time \textit{can} implicate an individual's reasonable expectation of privacy.”\footnote{128}{United States v. Graham, 846 F. Supp. 2d 384, 394 (D. Md. 2012).} While their views are not precedential, in the period since the decision was released in January 2012, some lower courts have discussed the idea that length of time implicates the Fourth Amendment, which suggests that the time length of the surveillance should be considered.

Cases after \textit{Jones}

Courts after \textit{Jones} have also recognized the temporal component in surveillance as part of its reasonableness analysis. In \textit{United States v. Skinner} the Sixth Circuit addressed continuous tracking of a suspect’s pay-as-you-go cell phone for three days.\footnote{129}{690 F.3d 772 (6th Cir.2012) (finding that because the suspect was tracked only on public roads and “the same information could have been obtained through visual surveillance” the suspect had no reasonable expectation of privacy in his location.).} While the court focused on \textit{Knotts} to find that there was no reasonable expectation of privacy,\footnote{130}{Id at 778 (“There is no inherent constitutional difference between trailing a defendant and tracking him via technology. Law enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system.”).} it also discussed how Justice’s Alito’s concerns in \textit{Jones} applied to the case.\footnote{131}{Id. at 780.} The court found that even though the advancement of technology makes Alito’s concerns over expectation of privacy valid, the three day search didn’t reach the same level of comprehensive tracking that violated the Fourth
Amendment in *Jones*. The three day search was within the “relatively short-term monitoring of a person’s movements on public streets [that] accords with expectations of privacy that our society has recognized as reasonable” because the tracking was “no more of a comprehensively invasive search than if instead the car” was tracked visually.

In *United States v. Powell*, the Eastern District of Michigan also discussed the temporal component of surveillance and distinguished the warrantless three day tracking in *Skinner* with warrantless tracking for almost a seven month period. The court found that tracking for nearly seven months in “this case does present the concerns regarding extreme comprehensive tracking raised in *Jones*.”

If Justice Alito’s assertion that “relatively short-term monitoring of a person’s movements on public streets accords with expectations of privacy that our society has recognized as reasonable” is true, then in following the decisions in both *Skinner* and *Powell*, the line between reasonable and unreasonable surveillance lies somewhere between three and twenty eight days. If that is where the line is, then any singular “ping” of a suspect or target’s geolocation data would be recognized by society as reasonable because such a search would last only a few seconds, far short of the three days *Skinner* found reasonable. It would also reveal solely the location of the target at that given moment, and not any of the information about

---

132 *Id* at 778
133 *Id*. (quoting *Jones*, at 964 (Alito, J., concurring)).
134 *Id*.
135 12-CR-20052, 2013 WL 1876761 at *10 (E.D. Mich. May 3, 2013) (finding that although tracking of GPS data for seven months exceeded an expectation of privacy and would require a warrant, the tracking data was still admissible under the good faith exception because it occurred before the *Jones* decision).
136 *Id*.
137 *Jones*, at 946. (citing *United States v. Knotts*, 460 U.S. 276, 281-82 (1983)).
138 *Skinner*, 690 F.3d at 780; and *Jones*, at 946.
person’s life Justice Sotomayor was worried about being disclosed through longer term surveillance.139

C. Third Party Surveillance

A third factor in determining the privacy interest in real-time geolocation data is to determine if the data was created solely by the Government’s own means or if it was created by a third party and given to the Government. When the Government creates the data solely by its own means, the factors described above apply, but where the Government obtains the geolocation data through a third party, then the question becomes whether or not the target has voluntarily conveyed that information to the third party.140

Obtaining the information from a third party trumps all other factors of reasonableness because it is inherent that a person has no expectation of privacy in information that has been voluntarily provided to a third party.141 As the Supreme Court found in United States v. Miller, when it decided there was no protection for the privacy of bank records:

the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to 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.142

139 Jones, at 956 (Sotomayor, J., concurring).
142 Miller, 425 U.S. at 443.
This also extends to information such as the location or address of a person if that information is conveyed voluntarily to the third party.\footnote{See Smith, 442 U.S. at 741-44; United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) (a person does not have an expectation of privacy in subscriber information provided to an internet provider, including their address).}

The most influential third party case on real-time geolocation surveillance is Smith v. Maryland, which involved the use of an electronic device to record the information from the third party in real time.\footnote{442 U.S. at 737.} In Smith, a woman was receiving obscene and threatening phone calls, and Smith was suspected of being the caller.\footnote{Id.} To determine if he was the caller, the telephone company, at the police’s request, installed a pen register at their central offices to record every number dialed from his home phone.\footnote{Id.} The pen register revealed that Smith placed a call to the woman.\footnote{Id. at 742.} The Supreme Court upheld the use of the pen register under the Katz test and found that there was no subjective expectation of privacy in the number he dialed because “all telephone users realize they must ‘convey’ phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed,” and also the phone company records the number which is seen on their monthly bill.\footnote{Id. at 741.} Further, the Court found that there was no content revealed in the numbers a person dials.\footnote{Id. at 742.} “Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even complete is disclosed by pen registers.”\footnote{United States v. New York Tel. Co., 434 U.S. 159, 167 (1977).}

Smith has great influence in determining the expectation of privacy in geolocation data, especially through third party acquisition of the data. Users of technology such as GPS devices,
cell phones, or smartphones, “similarly convey geolocation data to their telephone [or GPS] carriers.”151 As such, users cannot have a “belief that their location is somehow kept secret from telecommunication carriers and other third parties,”152 and therefore do not have a reasonable expectation of privacy to their location data.153 However, in order for the third party doctrine to apply, the information must be voluntarily provided, either through continued use or through the user directly.154 In fact, for tracking cell phone location, “all of the known tracking technologies may be defeated by merely turning off the phone.”155

Despite calls from some, like Justice Sotomayor in Jones,156 to move away from the third party doctrine with geolocation technology, Smith’s holding has been applied by some lower courts to find no reasonable expectation of privacy in cell phone and smartphone geolocation data. The Fifth Circuit found in In re Application for Historical Cell Site Data, that cell site information (“the antenna tower and sector to which the cell phone sends it signal”) was a business record and was voluntarily provided by the costumer, so there was no expectation of privacy in the information.157 The Eastern District of New York in In re Smartphone Geolocation Data Application found there was no privacy expectation in prospective data either because there was no subjective expectation of privacy in the geolocation data.158 That court pointed out that the smartphone shared its geolocation with social and commercial

---

152 Id.
153 Id.
154 Smith, 442 U.S. at 742,
156 Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring) (writing that it may be necessary to reconsider Smith in a digital age).
157 723 F.3d 600, 612-13 (5th Cir. 2013).
158 In re Smartphone, 2013 WL 5583711 at 14 (“it is clearly within the knowledge of cell phone users that their telecommunication carrier, smartphone manufacturer and others are aware of their location of their cell phone at any given time.’”).
applications.\textsuperscript{159} The District of Vermont, so far has been the first federal court to address third party real-time cell phone location data in \textit{United States v. Caraballo}.\textsuperscript{160} While the case was ultimately decided on different grounds, the court also noted there was no reasonable expectation of privacy in the real time data, finding “as a general proposition, cell phone location data is information a cell phone user voluntarily discloses to a third party in order to enable the cell phone user to send and receive calls.”\textsuperscript{161} Therefore, current case law supports the idea that there is no reasonable expectation of privacy when the geolocation data is conveyed as part of the ordinary business practices of the technology used.

Where the Government goes through a third party to obtain real-time geolocation data, the third party doctrine applies. So long as the data was provided voluntarily by the user or by the device being tracked, the Government’s acquisition of the data will be reasonable under the Fourth Amendment because the user will not have an expectation of privacy.

Society accepted expectation of privacy in geolocation data

From these three different components, there is a strong inclination that society will find that a person only has a limited expectation for privacy in their geolocation data. The short-term tracking of a person in order to learn only their whereabouts will therefore be reasonable under the Fourth Amendment. Such surveillance is a sense-augmenting technique because it only

\textsuperscript{159} \textit{Id} at 9 (the smartphone shared the geolocation data with applications: that track where the phone goes around a mall; allow police to find the phone when stolen; and a social application that shared the phone’s location with other users).

\textsuperscript{160} \textit{United States v. Caraballo, No. 5:12-cr-105, 2013 WL 4039028 (Aug. 7, 2013) (however, the court relied on the exigent circumstances to justify the warrantless cellphone pinging because the information was not voluntarily given off).}

\textsuperscript{161} \textit{Id.} at 18.
reveals the same information a person can obtain with their own eyes.\textsuperscript{162} The Government is blocked from tracking someone within their own home without a warrant,\textsuperscript{163} but geolocation data only reveals where a person is, and such information can be gathered from simply standing outside the house to see if the person is home.\textsuperscript{164} With regards to the length of the surveillance, it appears from Alito’s concurrence and the limited subsequent case law that society will accept a short-term tracking to determine someone’s location.\textsuperscript{165} Because \textit{Skinner} held that three days meets that short-term requirement,\textsuperscript{166} an instantaneous ‘ping’ to determine a person’s whereabouts would be short enough to be reasonable. Finally, if the Government goes through a third party to learn that information, and such geolocation data has been shared voluntarily with that third party, such as a cellular phone company or location based application, then the person has no expectation of privacy in that information.\textsuperscript{167}

\textbf{2. Subjective expectation of privacy in geolocation data}

Before a court can apply what society has deemed to be reasonable for geolocation, the individual being tracked must believe that his or her location is private, as the first prong of the \textit{Katz} test is “that a person [has] exhibited an actual (subjective) expectation of privacy.”\textsuperscript{168} Because this is a subjective component, it is hard to theorize what can be in a person’s mind at any given time. However, an idea of what a person will likely believe can be seen through how a

\begin{footnotes}
\item \textsuperscript{162} \textit{See Knotts, supra} note 59.
\item \textsuperscript{163} \textit{See Karo, supra} note 95.
\item \textsuperscript{164} \textit{See Knotts, supra} note 59.
\item \textsuperscript{165} \textit{Jones}, at 964 (Alito, J. concurring)
\item \textsuperscript{166} \textit{Skinner, supra} note 90.
\item \textsuperscript{167} \textit{See Smith, supra} note 140.
\item \textsuperscript{168} \textit{Katz} 389 U.S. at 361 (Harlan, J., concurring).
\end{footnotes}
person uses technology that can track their geolocation, and through the advancement and popularity of such technology.

Ultimately, as technology advances become more convenient, and more frequently used, the expectation of privacy a person has with that technology diminishes. With the availability of advanced technology, it appears that people are growing more accustomed to using devices that give off their geolocation and in providing such information to third parties, and sharing such information destroys their expectation of privacy in that information.\footnote{See Smith, supra note 140.} As such technology advances, people seemingly will have a better understanding that their location is being shared and that that information is no longer private.\footnote{See In re Application of the United States for an Order Authorizing the Release of Historical Cell-Site Information, 809 F.Supp.2d 113, 121 (E.D.N.Y 2011) ("Public ignorance as to the existence of cell-site-location records . . . cannot long be maintained.").}

It appears that this trend is already becoming true. There have been growing advancements in geolocation technology since the beeper used in \textit{Knotts},\footnote{Knotts, supra note 172} which allow the government to learn someone’s location. GPS, laptop computers, tablets, cell phones, and smartphones can all be used to determine someone’s location,\footnote{Alexandra D. Vesalga, Comment, \textit{Location, Location, Location: Updating the Electronic Communication Privacy Act to Protect Geolocation Data}, 43 \textit{Golden Gate U. L. Rev.} 459, 463 (2013).} and many of these devices inherently provide a third party with such location data. In \textit{Jones}, law enforcement had to physically attach a GPS device to Jones’s Jeep,\footnote{Jones, supra note 102.} but in the decade since that attachment, there has been a growing availability and use of both standalone and built-in GPS navigation systems.\footnote{Jamie Lendino, \textit{The History of Car GPS Navigation}, PC MAGAZINE (Apr. 16, 2012 1:39 PM), http://www.pcmag.com/article2/0,2817,2402755,00.asp.} Using this technology has already obtained results for law enforcement, as tracking a
built-in GPS navigation system played a key role in locating the alleged Boston Marathon bombers.\textsuperscript{175}

In addition to GPS navigation systems, the government can also obtain geolocation data from both cell phones and smartphones. Both cell phones and smartphones still make calls the same way, and they can each be traced through their cell-site location.\textsuperscript{176} In order to ensure that a call can be received, both cell phones and smart phones “constantly relay their locations to cellular towers . . . roughly every seven seconds when the cell phone is turned on.”\textsuperscript{177} When a call is received or made, the provider locates the user based on the nearest tower.\textsuperscript{178} The user’s location can be determined based on the strength of the signal from the tower.\textsuperscript{179} Although the third party doctrine applies here, because this information is gathered by the cell service provider, the growing use of these phones makes it difficult for the public not to realize that their location is not private.\textsuperscript{180} A Pew Research Center survey in May 2013 found that cell phones are now being used by 91\% of the adult population in America, up from only 65\% in 2004.\textsuperscript{181} In fact “the cell phone is the most quickly adopted consumer technology in the history of the world.”\textsuperscript{182}

\textsuperscript{176}Vesalga, 43 GOLDEN GATE U. L. REV at 466 (“All mobile service providers collect cell site data as part of routing and transmitting phone calls”).
\textsuperscript{177}Kevin McLaughlin, Note, The Fourth Amendment and Cell Phone Location Tracking: Where are We?, 29 HASTINGS COMM. & ENT. L.J. 421, 426 (2007).
\textsuperscript{178}I\textsuperscript{d}.
\textsuperscript{179}I\textsuperscript{d}.
\textsuperscript{180}See In re Application of the United States for an Order Authorizing the Release of Historical Cell-Site Information, 809 F.Supp.2d 113, 121 (E.D.N.Y. 2011) (“Public ignorance as to the existence of cell-site-location records . . . cannot long be maintained.”).
\textsuperscript{181}Lee Rainie, Cell Phone Ownership Hits 91\% of Adults, PEW RESEARCH CENTER (Jun. 6, 2013) http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/.
\textsuperscript{182}I\textsuperscript{d}. 
The same survey found that 61% of those cell phone owners use a smartphone, which means that 56% of adult Americans use a smartphone.\textsuperscript{183}

Smartphones, although they make phone calls the same way as regular cell phones, may provide even more opportunities to trace a person’s location. While each type of mobile phone constantly searches for a signal through cell towers, the Government cannot merely outright ping a phone, and the location must be received from a call that was made or received.\textsuperscript{184} With smartphones, a user can install applications, colloquially known as apps,\textsuperscript{185} on to the phone. Many of these apps continue to run even if the smartphone is not making a call, and can constantly collect data on a person’s location.

Many of these apps are location-based services, “applications that provide information to users based on their location.”\textsuperscript{186} These applications offer services based on your location such as GPS navigation, business or restaurant finders, weather, or social networking.\textsuperscript{187} Installing and using such apps allows the company that produced the app to gather more information about the user than just their location.\textsuperscript{188} A person’s location “may be used once for a single purpose, or it may be stored or combined with other information to produce a history of the consumer’s activities or a more detailed profiled for advertising or other purposes.”\textsuperscript{189} In fact, a location-based service application can compile the “mosaic” of a person’s life that both Alito and

\begin{thebibliography}{9}
\bibitem{184} See Caraballo, \textit{supra} note 156.
\bibitem{187} \textit{Id.}
\bibitem{188} \textit{Id.} at 3.
\bibitem{189} \textit{Id.}
\end{thebibliography}
Sotomayor were afraid of in Jones,190 and sell it to anyone191 or the Government can obtain such information without a warrant because of the third party doctrine.192

Additionally, the growing number of smartphone app users diminishes any expectation a person would have to keep their information private. As of March 2013, there are more than 1.5 million apps available for Apple or Google smartphones, the two most popular brands, and the average smartphone has 41 apps.193 This signifies that the common person has voluntarily lowered their expectation of privacy with their geolocation data because they are constantly sharing their locations with these third party location-based service apps.

With social location based services, the person’s expectation of privacy, is even less, because they voluntarily provide details of their whereabouts.194 Social media networks such as Facebook or Foursquare allow a person to check into any place they are at.195 In fact, the whole point of Foursquare is “to share and save the places you visit.”196 By voluntarily ‘checking in’ to a location, the person has voluntarily prevented any claim of an expectation of privacy in their geolocation at that place.

Statistical researchers have already begun to look into the extent of the information this growing use of location-based technology reveals, and the results are startling. Finnish researchers developed an algorithm that accurately reveals the transportation method a person

---

190 Jones, discussion supra part II 1. B.
191 Nick Lane, “Mobile geo-location advertising will be a big number in 2015,” MOBILESQUARED 7 (2012), available at http://adfonic.com/wp-content/uploads/2012/03/geo-location-white-paper.pdf (the geolocation of about 50% of all iPhone and Android smartphones are available to advertisers).
192 See Smith, 442 U.S. at 735.
194 See Ozer, supra note 186, at 1.
195 Id.
uses based on GPS and accelerometer data created by smartphones.\textsuperscript{197} Studies have also found that plotting the location and time of cell phone calls and text messages can reveal a vast array of information about a city’s urban planning.\textsuperscript{198} A 2011 study by AT&T Labs plotted the aggregate of this cellular traffic for two months in and around Morristown, New Jersey, a New York suburb of about 20,000 people.\textsuperscript{199} The study used this data to create a laborshed map of the location of workers in the town, and the results were remarkably similar to the laborshed map created using the 2000 U.S. Census data.\textsuperscript{200} This data was also used to identify patterns of life in the city, such as when school lets out or when bars close.\textsuperscript{201}

Yet another study found that “human mobility traces are highly unique,” and a person’s identity can be determined based solely on their movements.\textsuperscript{202} This study found that by selecting as little as four randomly selected spatial-temporal points (approximate location and approximate time the cell phone is in use) could be used to uniquely identify over 95\% of the

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{197} Samuli Hemminki et al., Accelerometer-Based Transportation Mode Detection on Smartphones, HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY (2013), available at http://www.cs.helsinki.fi/u/shemmink/Transportation/hemminki13transportation.pdf (evaluation based on data collected over 150 hours from 16 individuals in 4 different countries using varying models of Samsung Galaxy S smartphones.).
\item \textsuperscript{199} \textit{Id} at 1-2 (collected 15 million voice records and 26 million text message records for 475,000 unique phones of only AT&T subscribers).
\item \textsuperscript{200} \textit{Id}. at 4-5 (noting that the maps were not identical because they only reflected activity of only AT&T subscribers and the 2000 Census data was over a decade old).
\item \textsuperscript{201} \textit{Id} at 6.
\item \textsuperscript{202} Yves-Alexandre de Montjoye Et al., Unique in the Crowd: The Privacy Bound of Human Mobility, SCIENTIFIC REPORTS 1, 5 (2013), available at http://www.nature.com/srep/2013/130325/srep01376/pdf/srep01376.pdf (The results were based on an anonymized cell phone data set with information for \~1.5 million users, and was created by plotting the location of the cell tower each time the user made or received a call or text message).
\end{itemize}
\end{footnotesize}
population, and 50% of the population could be identified through using only two points.\textsuperscript{203} In other words, it is extremely unlikely that two people will be in the exact same four locations at the exact same time.\textsuperscript{204} In comparison fingerprints require twelve independent points for identification.\textsuperscript{205} The researchers also noted that these four points could be obtained through publicly available information such as home address, office address, or geo-localized posts to the internet.\textsuperscript{206}

These studies show that through the increase use of technology, particularly smartphone, the average person has less of an opportunity to claim an expectation of privacy in their geolocation against Government surveillance. An individual is sharing more and more of themselves with third parties through using technology, and sometimes are even voluntarily providing information to the public. Therefore, if the Government seeks to obtain a person’s geolocation through such technology, then the third party doctrine clearly allows it.

Conclusion

Moving forward, the largest hurdle for a protection of privacy in one’s location is the third party doctrine. In Jones, in both the Alito and Sotomayor concurrences five justices were fearful that the Government could develop a mosaic of a person’s life through collecting real-time electronic geolocation data.\textsuperscript{207} Yet, with the studies performed using the data already given off by current technology it appears that such a mosaic is readily available to the companies who

\textsuperscript{203} Id. at 2.
\textsuperscript{204} Id.
\textsuperscript{205} Id.
\textsuperscript{206} Id.
\textsuperscript{207} See Jones, 132 S. Ct. at 954-64.
run cell phone and location-based apps,208 and through the third party doctrine, an individual will have no expectation of privacy in that data.209 Consequently, the Government can acquire such data without a warrant. Therefore Justice Sotomayor’s comments might be true, that to readily address the protection of privacy in new technology a re-thinking of the third party doctrine may be needed, at least for the collection and aggregation of long-term geolocation data.210 However, with sites such as Facebook, Foursquare, and Twitter, all of which allow the user to declare to not only to their “friends” but to the world where they are, a re-thinking of the third party doctrine might be too late. It appears that society has already accepted that a short-term, real-time geolocation trace of a person’s location does not infringe upon their Fourth Amendment right to privacy.

208 See de Montjoye, supra note 202.
209 See Smith supra, note 144 at 742.
210 Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring) (“more fundamentally it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.”).