SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 27 FALL 2012 ARTICLE 1, PAGE 1

Cell-Site Location Data and the Right to Privacy

Jen Manso

I. Does a Privacy Right Still Exist?

The recently decided Supreme Court case *United States v. Jones* underscores the growing debate over privacy rights and government surveillance in the digital age.[1] A cell phone user can be tracked in a few different ways including the global positioning system ("GPS") technology installed on their phone similar to the GPS device used in *Jones* and also through cell-site tracking via triangulation. Whether this information, which is stored by the cell phone user's wireless service provider is available to anyone is a question of privacy rights and how the Courts want to interpret them. While this paper focuses mainly on location data recovered as a result of cell-site tracking, reference to GPS technology and the governing law are important because the import of the technologies are so similar as they are used for the same purposes and sometimes used together to gather location data.

As of 2005, mobile phones were almost as prevalent as conventional phones with over 195 million cellular subscribers in the United States alone.[2] By advertising

[1] *See* United States v. Jones, 132 S.Ct. 945 (2012).

[2] Matt Richtel, *Live Tracking on Mobile Phones Prompts Court Fights on Privacy*, N.Y. TIMES, Dec. 10, 2005, http://www.nytimes.com/2005/12/10/technology/10phone.html.

applications that turn cell phones into more precise global positioning devices, wireless phone companies exploit cell phones' tracking abilities.[3]

Naturally, technology available to the public is also available to government. Thus, it is of no surprise that law enforcement agencies would want to take advantage of this technology too.[4] As a result, more courts have been asked to determine what legal standard applies when the government wants to use this technology to gather intelligence by tracking an individual.[5] The question becomes, does the government need probable cause or something less?

II. Cell Phone Location Data Has Various Uses.

Cell phone location data (cell cite location data) can be used for many different purposes. In the private sector, one can trace their lost or stolen cell phone from software uploaded on their phone and downloaded on a separate device.[6] From the convenience of their cell phone, the user can access driving directions to a desired location from their current location. A long-haul trucking company can keep track of their fleet of trucks and a taxicab company can determine where their drivers are at any time and in any location.

---

[3] Ritchell, *supra* note 2.

[4] *Id*.

[5] *Id.*

[6] Bay City News Service, *Tracking Software leads Oakland police to stolen cell phone, arrests*, Silicon Valley, MercuryNews.com (posted February 17, 2012, updated February 21, 2012)(last visited February 21, 2012) available at http://www.mercurynews.com/breaking-news/ci_19993478.

At the government's end, cell phone location data can be used to determine a precise location from where a 911 emergency phone call was made, responding to the victims faster than ever before.[7] In fact, the Federal Communication Commissions ("FCC") has been a large influence in improving the precision and encouraging the development of cell-site location data.[8] The Wireless Communications and Public Privacy Act of 1999 provided the FCC with this foundation and requires wireless telephones to be equipped with locating technology and requires service providers to provided the coordinates - latitude and longitude (within certain ranges) for all emergency calls dialed from a cellular phone.[9] A typical cell phone "will reveal between 20 and 55 location points a day."[10] This data is sufficient to plot the target's movements hour by hour over an extended period of time.[11] "If registration data[12] were also collected by the provider and made available, such records would track the user on a minute by

---

[7] Public Safety and Homeland Security Bureau, *Enhanced 9-1-1 Wireless Services,* FCC, available at http://www.fcc.gov/pshs/services/911-services/enhanced911/Welcome.html; Recent Development, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 308 (2004); *see also Understanding Wireless Telephone Coverage Areas*, FCC Consumer Facts, *available at* www.fcc.gov/cgb.

[8] *See* Recent Development, *supra* note 7, at 308-09.

[9] *See* 47 C.F.R. § 20.18(h)(1) (2008); *see* Ken Wallentine, J.D., *Cell-Site Location Evidence: A New Frontier in Cyber-Investigation*, 2 AELE MO. L. J. 401, 403 (February 2011).

[10] *Cellular Phone Evidence: Cell-Site Location Data*, 13 No. 1 Crim. Prac. Guide 3 (January/February 2012) (citing In re U.S. for Historical Cell-Site Data 747 F.Supp.2d. 827, 835 (S.D. TX 2010)[hereinafter *Cellular Phone Evidence*].

[11] *See Cellular Phone Evidence*, *supra* note 10 at 1.

[12] *See* Chamberlain, *infra* note 59 at 1747 and accompanying text; *see* McLaughlin, *infra* note 59 at 426 and accompanying text.

minute basis, compiling a continuous log of [a person's] life, awake and asleep."[13] Government officials have used the data available from tracking cell phones to solve a variety of crimes.

For example, in California, two robbery suspects were located and detained after using a stolen cell phone equipped with Apple's cell phone tracker software.[14] On a larger scale and helping to fight the war on terrorism, the suspect in the 2005 failed suicide bombings was located after he made calls from his cell phone.[15] In another example, the famous Scott Peterson case also presents another example of when cell-site location data was used to locate Peterson and bring about justice.[16]

---

[13] *See Cellular Phone Evidence*, *supra* note 10 at 1.

[14] Bay City News Service, *Tracking Software leads Oakland police to stolen cell phone, arrests*, Silicon Valley, MercuryNews.com (posted February 17, 2012, updated February 21, 2012)(last visited February 21, 2012) at http://www.mercurynews.com/breaking-news/ci_19993478. The phone was traced by software that one of the victims had installed on his iPad. *Id.* The software was designed to track the phone for this very purpose. *Id.* With this software, the police tracked down two suspects and recovered a vehicle filled with additional stolen goods allegedly used in several additional robberies. *Id.*

[15] *Tracking a suspect by mobile phone*, BBC NEWS (Wednesday, August 3, 2005) at http://news.bbc.co.uk/2/hi/technology/4738219.stm (last accessed January 3, 2012). The Italian police were able to monitor the suspect even though he changed his SIM card while he was on the move. *Id.* The reason is this - a cell phone has two identifiers: (1) the IMSI (International Mobile Subscriber Identity) number, which reveals the user's country code, user account, network code and telephone number, (2) the IMEI (International Mobile Equipment Identity) number which identifies the handset's number "and remains constant even if the SIM card is changed." *Id.* These numbers are reported to nearby base stations. *Id.* Once the information from several of the stations is collected, a geographical location is determined by a triangular calculation between the base stations. *Id.* This calculation can pin point a user's location within a few hundred meters if in an urban area. *Id.*

[16] *See* Diana Walsh & Stacy Finz, *The Peterson Trial: Defendant Lied Often, Recorded Calls Show; Supporters Misled About Whereabouts*, S.F CHRON., Aug. 26 2004, at B1, *available at* http://www.sfgate.com/cgi-bin/article?f=/c/a/2004/08/26/BAG458EJ3S1.DTL.

III. Cell Site Location Data Raises Concerns About Privacy.

Government accessibility to cell phone tracking technology has stirred quite a bit of controversy[17] with concerns about privacy and civil rights at the core of the debate.[18] Specifically, the debate centers over whether use of cell phone tracking technology to gather the whereabouts or "location data" of a suspect necessitates a pre-determination of probable cause to satisfy a warrant application, or if legal use of such technology is satisfied by something less.[19] If the use of cell phone tracking technology to obtain the location data of a suspect is considered a search by definition of the Fourth Amendment and the proceeding years of precedent, then a predetermination of probable cause is necessary, and, only where an exception lies, will the warrantless search pass constitutionality. However, if such use of cell phone location data falls outside the scope of a Fourth Amendment search, the need for probable cause disappears.

---

[17] *See Cellular Phone Evidence*, *supra* note 10 at 1 and accompanying text; also *see* Jennifer Grankick, *Can You Track Me Now? Not without a Warrant!*, Law Across the Wire and Into the Cloud Recent Developments in Internet Law *available at* http://blog.zwillgen.com/2011/08/26/can-you-track-me-now-not-without-a-warrant/(last accessed March 3, 2012); *cf.* Bob Brown, *Cornell Prof Warns iPhone, iPad users: "We are selling our privacy," Says cell phone users need to take privacy into account when designing systems*, Network World, April 21, 2011, *available at* 2011 WLNR 8023612; *cf.* David Kravets, Court OKs Warrantless Cell-Site Tracking, Wired.com *available at* http://www.wired.com/threatlevel/2010/09/cell-cite-data/.

[18] J.R. Labbe, *Fortworth Police tracking-tracking system deserves public scrutiny*, Star Telegram at http://www.star-telegram.com/2012/02/27/3767543/fort-worth-police-cellphone-tracking.html (Posted Monday February 27, 2012)(last visited February 28, 2012); *see generally* Am. Civil Liberties Union v. U.S. Dept. of Justice, 655 F.3d 1 (2011).

[19] *See* Richtel, *supra* note 2.

As evidence of the debate in action, some police departments plan on using the technology *after* a determination of probable cause, upon issuance of a warrant.[20] This would be the proper procedure if use of cell cite location data is considered a Fourth Amendment search. If not, policy concerns are worth considering: the probable cause and warrant requirements might present unnecessary hurdles for law enforcement to jump through also, the processes for developing probable cause and applying for a warrant will needlessly use state and federal resources. One former Manhattan prosecutor stated that "[i]t can have a major impact, . . . [i]f I am on an investigation and I need to know where somebody is located who might be committing a crime, or, worse, might have a hostage, real-time knowledge of where this person is could be a matter of life or death."[21]

However, it seems that other departments plan to use the technology to "assist in locating, identifying, and *developing* probable cause and apprehending priority offenders."[22] While to some, this violates privacy at its core; if the use of cell-site location data is not a Fourth Amendment search, use of the location data to "develop" probable cause will be perfectly legal subject to state and federal statutes aimed at

[20] *See In re U.S. for Historical Cell-Site Data* 747 F. Supp. 2d 827 (S.D. TX 2010); *see also Cellular Phone Evidence*, *supra* note 10, at 1.

[21] *See* Richtel, *supra* note 2.

[22] Labbe, *supra* note 18 (emphasis added). One city recently found itself in a $184, 319.00 debate over whether the city council should approve the Police Department's application for a comprehensive cell-phone tracking system similar to that used by the F.B.I. and U.S. Marshalls Service. *Id.* Privacy and civil rights activists were infuriated after reading memo offered before the city council in support for the tracking system. *Id.* In part the memo stated: "The Police Department will use the KingFish System, a portable tracking-tracking system, to assist in locating, identifying, developing probable cause and apprehending priority offenders." *Id.*

limiting this.[23] According to some government officials, the applicable standard is laid out in the 1994 amendment to the Stored Communication's Act.[24] According to this statute, the government is only required to show "specific and articulable facts" that demonstrate that the records sought are "relevant and material to an ongoing investigation."[25] This standard is much lower than a showing of probable cause.[26] The Pen Register Act has also been used to give magistrates authority to grant applications with something less than probable cause but other limitations do apply.[27] In recent cases, prosecutors have "unsuccessfully argued that the expanded police powers under the USA Patriot Act could be read as allowing cell phone tracking under a standard lower than probable cause."[28] The policy concerns here are best characterized by Justice Douglas when he stated that "[i]f the Warrant Clause were held inapplicable[,] . . . then the federal

---

[23] *See* Ian James Samuel, *Warrantless Location Tracking*, 83 NYU L. REV. 1324, 1330-31 (Oct. 2008).

[24] *See* Richtel, *supra* note 2.

[25] 18 U.S.C. §§ 2701-2711 (2000); *see also* Richtel, *supra* note 2.

[26] *Id.*

[27] 18 U.S.C. 3121(a); Interestingly, but outside the scope if this paper, the language of "a separate statute, the Communications Assistance for Law Enforcement Act (CAOEA) says that no order issued 'solely pursuant' to the Pen Register Act may disclose the physical location of the subscriber." *See* Samuel, *supra* note 23, at 1333 (arguing that the act leads one to believe that this standard is only applicable when the statute is used in conjunction with another law which remains unclear); *see* 47 U.S.C. § 1002(a)(2)(2000). The statute states: "[W]ith regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number);" *see* Samuel, *supra* note 23, at 1333.

[28] Richtel, *supra* note 2.

intelligence machine would literally enjoy unchecked discretion."[29] In support of this argument, one South Texas Magistrate argues that "[p]ermitting surreptitious conversion of a cellphone into a tracking device without probable cause raises serious Fourth Amendment concerns especially when the phone is monitored in the home or other places where privacy is reasonably expected."[30]

IV. Cell Phones Can Reveal Data Through Different Technologies.

A. Historical data and real-time data are different in time but related in technology.

When dealing with digital surveillance, the government can choose from two different types of data: historical data and data in real time. Historical data is, in simple terms, data in the past.[31] It is data that will reveal where a person has been at a certain time and place.[32] Often historical data reveals itself in a single form such as where a single outgoing telephone number was dialed at a single point in time.[33] This data is arguably governed by the Stored Communications Act or even the Pen Register Statute,

[29] United States v. U.S. Dist. Court for E. Dist. of Mich., 407 U.S. 297, 325 (1972)(Justice Douglas' concurring opinion stated that "even the risk of exclusion of tainted evidence would here appear to be of negligible deterrent value, inasmuch as the United States frankly concedes that the primary purpose of these searches is to fortify its intelligence collage, rather than to accumulate evidence to support indictments and convictions. If the Warrant Clause were held inapplicable here, then the federal intelligence machine would literally enjoy unchecked discretion.").

[30] In re Application for Pen Register and Trap/Trace Device with Cell-Site Location Authority, 396 F.Supp.2d 747, 765 (S.D. Tex. 2005).

[31] *See* Wallentine, *supra* note 9, at 401, 406, 408.

[32] *Id.* at 404.

[33] *See* Wallentine, *supra* note 9, at 404.

and is therefore, if a distinction can be made, arguably less deserving of heightened legal scrutiny than real time data (also known as data in motion).[34] Real time data is present time information and is arguably governed by the "super warrants" of The Wiretap Act.[35] This data will typically reveal a user's location as they are moving from one moment to the next. Cell-site location data is capable of providing historical "pen register type" data, as well as real-time, moment-to-moment monitoring. While GPS is most known for its real-time surveillance, both technologies offer discrete surveillance.[36] "The distinction between cell-site data and information gathered by a tracking device has practically vanished."[37] The goal of the investigation will most likely determine which data law enforcement will choose to apply for. In some cases, law enforcement might find it useful to apply for both.

B. It is important to understand why and how digital surveillance became so available and the differences between the several options.

Cellular service providers, motivated by the Federal Communications Commission ("FCC"), have been providing location information in the context of 911 calls for years.[38] The

[34] *See* Wallentine, *supra* note 9, at 404, 407.

[35] *See* 18 U.S.C. § 2518 (1998). The Wiretap act, on top of a showing of probable cause demands compliance with other procedures as well. This would be the strictest showing.

[36] See Wallentine, *supra* note 9, at 401, 403-06, 408.

[37] *See* Richtel, *supra* note 2.

[38] *See* Recent Development, *supra* note 7, at 308.

FCC recognized the need for location information, or the details of an individual's whereabouts, as more and more people began making 911 calls from their cell phones rather than their wired telephones.[39] Among the advancing technologies, service providers typically use one of the following three technologies to "pinpoint" the locations of their subscribers: nearest sensor technology, global positioning system ("GPS") technology, or signal triangulation.[40]

1. Nearest sensor technology fails to provide law enforcement with desired precision.

The simplest and most commonly used technology by wireless service providers is nearest sensor technology.[41] Nearest sensor technology provides location information by determining the single access point or cellular base station to which a cell phone is associated.[42] This technology bases its location information on an assumption that the sensor that the cell

---

[39] Recent Development, *supra* note 7, at 308 (stating that "the difficulties presented by cell phone emergency calls led the Federal Communications Commission ("FCC") to set a deadline after which cell service providers must supply location information so that emergency callers can be located within 150 meters").

See also Federal Communications Commission, *Wireless 911 Services, Guide* at http://www.fcc.gov/guides/wireless-911-services (last visited Feb. 3, 2012) (detailing how services providers must comply by providing a "list of counties and portions of counties, that they seek to exclude from the location accuracy requirements . . . because of either heavy forestation or the inability to triangulate a caller's location); *see also* 911 Service, 47 C.F.R. § 20.18 (2004) (mandating licensees to "achieve 95 percent penetration of location-capable handsets among [their] subscribers" by December 31, 2005).

[40] *See* Recent Development, *supra* note 7, at 308.

[41] Joanie Wexler, *All About Wi-Fi Location Tracking: Finding things is easy with Wi-Fi,* TECHWORLD (April 4, 2006), http://features.techworld.com/mobile-wireless/2374/all-about-wi-fi-location-tracking/ (last visited Feb. 3, 2012).

[42] *Id.*

phone is associated with is the closest sensor to the cell phone.[43] Working within a three dimensional diameter of the 360-degree radiation 'cell' surrounding the sensor, the base station then computes how far the signal radiates.[44] This technology is the least precise of all the location tracking technologies but is nevertheless utilized.[45]

2. Global Positioning Technology provides the most precision but is not as accessible to law enforcement as other available resources.

Global positioning technology is "an aerospace technology that uses satellites and ground equipment to determine position anywhere on earth."[46] GPS technology enables providers to precisely identify the location of a GPS enabled cell phone anywhere in the world.[47] In a simple explanation, "GPS works by measuring the time it takes for a signal to travel the distance between satellites and a cell phone's GPS chip. When the GPS chip receives four synchronized signals from GPS satellites, it can calculate a three-dimensional location that is accurate within 20 meters."[48] In some cases, GPS technology "combine[s] triangulation with a measurement

[43] Wexler, *supra* note 41.

[44] *Id*.

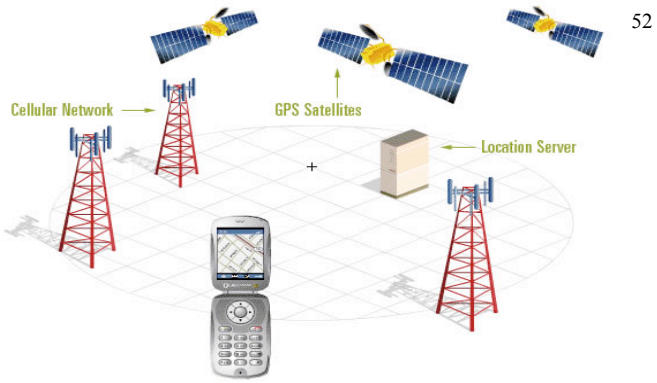
[45] *Id.*

[46] Smithsonian National Air and Space Museum, *GPS: A New Constellation*, *available at* http://www.nasm.edu/gps/ (last visited Feb. 3, 2012) [hereinafter Smithsonian]. Recent Development, *supra* note 7, at 308-10.

[47] *See* Recent Development, *supra* note 7.

[48] Smithsonian National Air and Space Museum, How Does GPS Work?, at http://www.nasm.si.edu/exhibitions /gps/work.html (last visited Feb. 3, 2012); *see* Recent Development, *supra* note 7; *see* Smithsonian National Air and Space Museum, GPS In More Detail, at http://www.nasm.edu/gps/spheres.html (explaining the "four synchronized signals as

called time difference of arrival (TDOA) over a network of satellites"[49] TDOA measures the relative time delay of signals arriving and received by different cell towers and is compatible in a network of triangulation.[50] "Because time is proportional to the distance traveled, the distance to each sensor within range can be estimated and, consequently, the location of the [cell phone user]."[51] Apple's iPhone and the Android network both use GPS technology for tracking the stolen or lost phones, and GPS technology, while making its way into the smart phone arena, is the least employed technology of the three mentioned in this article because it is the most expensive and not yet available on all cellular phones.



[52]

spheres: "Three spheres are necessary to find position in two dimensions, four are needed in three dimensions."); Recent Development, *supra* note 7, at 308-10.

[49] *See* Wexler, *supra* note 41.

[50] Wexler, *supra* note 41.

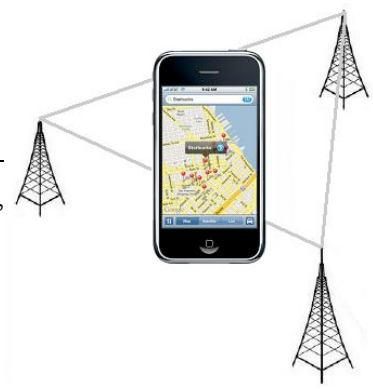
[51] *Id.*

[52] *A GPS (Assisted GPS)*, NAVI-GADGET.COM, http://www.navigadget.com/wp-content/postimages/2007/01/a-gps-944.jpg (last visited Nov 2011). A GPS is different from regular GPS because it is supported by an assistance server that helps share the tasks of a single GPS network. *Id.* This speeds up the process. *Id.* Mobile networks are often the go to for Assistant Servers. *Id.*

3. Triangulation is the most common cell phone tracking technology used by law enforcement authorities.

The focus of the article is on the privacy rights akin to information received from cell-site location information collected by third party service providers. This technology most commonly comes in the form of signal triangulation. Like nearest sensor technology and GPS technology, signal triangulation technology is also capable of locating the position of the cell phone user, but instead of obtaining the user's location by assessing the radius surrounding a single cellular base station or receiving a direct satellite communication, detailed positioning information is obtained from a cell service provider's service towers.[53] Cell towers are also known as cellular base stations or cell-sites.[54] The information gathered from these cell-sites is referred to as cell-site location information.[55] "Triangulation," for purposes of cell-site location information, measures the angels between three or more nearby cell-sites.[56] The point at where the angles intersect is calculated as the client location or the position closest to the device, and is usually within 50 meters of the actual cell phone location.[57]

[58]



[53] *See* Recent Development,

[54] *Id.*

[55] *Id.*

[56] *See* Wexler, *supra* note 41.

[57] *Id.*

[58] Nabanita, *iPhone records your position on the sly*, GadgetsLane.com(April 25, 2011) at http://www.gadgetslane.com/wp-content/uploads/2011/04/iPhone-with-GPS.jpg (last accessed February17, 2012).

The process where cellular phones communicate with nearby service towers is called registration.[59] As long as the cell phone is powered on, the process of communication remains continuous and automatic.[60] In other words, the cellular user does not have to do anything for the communications between the towers to repeatedly occur.[61] Thus, despite cell phone users not dialing out or answering incoming calls, cell phones continue to communicate with the nearest cell tower to "register."[62] For identification purposes, each cell phone has two different types of numbers: a Mobile Identification Number ("MIN") and an Electronic Serial Number ("ESN").[63] A MIN is the ten-digit number another caller dials to call a cell phone--in plain terms this is the caller's telephone number.[64] By contrast, an ESN is a unique, unchangeable number assigned by

[59] Patrick T. Chamberlain, *Court Ordered Disclosure of Historical Cell-Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH.& LEE L. REV. 1745, 1747 (Fall 2009); *see* Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where are We?,* 29 HASTINGS COMM. & ENT. L.J. 421, 426 (2007) (detailing the process of "registration," in which cellular phones "relay their locations to cellular towers").

[60] Chamberlain, *supra* note 59, at 1747; McLaughlin, *supra* note 59, at 426 (noting that registration "occurs roughly every seven seconds when the cell phone is turned on.").

[61] Recent Development, *supra* note 7, at 309 ("Even when users are not making or receiving calls, cell phones communicate with the nearest cell tower to register.").

[62] Recent Development, *supra* note 7, at 309.

[63] *Id.*

[64] *Id*.

the manufacturer.[65] To maintain outgoing calls and ensure delivery of incoming calls, the cell phone device must periodically notify the network service provider of the call locations.[66] As soon as the cell phone "registers" its MIN and ESN with a particular cell, the service provider then sends incoming calls directly to the cell.[67] As a cell phone user continues to travel to new locations, the cell phone continues to re-register.[68] However, once the cell phone is powered off, "the registration with a particular cell expires."[69] From this continuous communication, cellular service providers collect detailed information regarding the tower locations relied upon by the cellular users, "which in turn can provide a relatively detailed picture of those users' geographic whereabouts."[70]

As technology revealing location information has advanced, law enforcement has found great value in its use beyond responding to 911 calls. As previously discussed, law enforcement has used GPS technologies to track drug traffickers, terrorists and killers, law enforcement has also turned to cell-site location data technologies to help with catching criminals and in some cases saving lives.[71] In simple terms, the policy question resides in the tradeoffs between the

---

[65] *Id.*

[66] *Id*.

[67] Recent Development, *supra* note 7, at 309.

[68] *Id*.

[69] *Id*.

[70] Chamberlain, *supra* note 59, at 1747; *see also Cellular Phone Evidence*, *supra* note 10, at 1.

[71] *See generally* United States v. Jones, 132 S.Ct. 945 (2012) (involving the government's use of GPS technologies to establish probable cause to arrest a suspected drug trafficker); (discussing how the government's use of GPS technology helped catch Scott Peterson in the Lacy Peterson Murder); *see also* Recent Development, *supra* note 7, at 310-11; *see also* Chamberlain, *supra* note 59, at 1747 ((stating that CSLI has great utility for law enforcement)(citing Recent Development, *supra* note 7, at 310-11)).

protections of digital surveillance and Fourth Amendment Privacy Rights. How much privacy is society willing to give up?

IV. The Fourth Amendment Governs Surveillance Techniques.

If the government wants to learn about a person, it is equipped with an array of resources to choose from. Aside from the traditional "steak-out," advances in technology have led to surveillance options like wiretaps for telephonic and computer communication, beepers, pen registers, GPS, and cell-site location tracking. However, it must use these resources within the parameters of the law.[72]

A. What are Fourth Amendment privacy rights?

The Fourth Amendment is the most important law that governs the employment of these resources and states that:

> "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[73]

---

[72] Electronic Frontier Foundation, *Surveillance Self-defense: What Can the Government Do?* https://ssd.eff.org/your-computer/govt (last accessed January 3, 2012).

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

A seizure is said to occur when the government takes complete control over an item or person.[74] And, until recently, a search was defined as "any intrusion into something in which one has a reasonable expectation of privacy."[75] The Fourth Amendment's requirement of reasonableness mandates that all searches and seizures that violate this requirement can only proceed upon application and receipt of a validly executed search warrant.[76] A warrant is considered valid upon a determination of probable cause, which is then presented to and approved by a "neutral and detached decision maker."[77] But for an exception to the general warrant requirement[78], the evidence recovered as a result of an unlawful search or seizure will not survive the vigors of suppression.[79] Though in many situations the exclusionary rule[80] proves effective in deterring unlawful government conduct, the deterrent effect might not be as potent in situations involving certain surveillance techniques like wiretapping or cell-site

[74] Electronic Frontier Foundation, *supra* note 72.

[75] *Id.*

[76] *Id.*

[77] *Surveillance Self-defense: Search Warrants,* ELEC. FRONTIER FOUND., https://ssd.eff.org/your-computer/govt/warrants (last accessed January 3, 2012).

[78] *Surveillance Self-defense: Warrantless Searches,* ELEC. FRONTIER FOUND., https://ssd.eff.org/your-computer/govt/warrantless (last accessed January 3, 2012) (wherein exceptions include: the plain view doctrine, exigent circumstances, and the harmless error rule).

[79] Electronic Frontier Foundation, *supra* note 72.

[80] The exclusionary rule mandates that evidence obtained in violation of the Fourth Amendment shall be excluded but for an exception to the rule. *See* Weeks v. United States, 232 U.S. 883 (1914) (holding that a man's house is his castle protected from unlawful searches and seizures, seized lottery tickets collected as a result could not be used as evidence). This was one of the first applications of the exclusionary rule. *Weeks v. United States*, OYEZ *available at* http://www.oyez.org/cases/1901-1939/1913/1913_461 (last visited February 4, 2012).

location data.[81] Relevant to this discussion is the historical development of the Fourth Amendment's application particularly as it applies to surveillance.

B. To understand current Fourth Amendment jurisprudence, it is important to understand past Fourth Amendment jurisprudence.

The United States Supreme Court recently reminded the government that the Fourth Amendment was originally founded in concepts of property law.[82] Resolving whether the installation of a GPS device on a target's vehicle for the purpose of monitoring the vehicle's movements constitutes a search in violation of the Fourth Amendment, Justice Scalia expressed "no doubt that such a *physical intrusion* would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[83] Rooted in concepts of traditionalism and framers' intent, Scalia quotes the foreshadowing of Lord Camden from the famous 1765 case *Entick v. Carrington*.[84]

> Lord Camden expressed in plain terms the significance of property rights in search-and-seizure analysis: [O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbor's close without his leave; if he does

[81] United States v. United States District Court, 407 U.S. 297, 325 (1972) (Justice Douglas' concurring opinion stated that "even the risk of exclusion of tainted evidence would here appear to be of negligible deterrent value, inasmuch as the United States frankly concedes that the primary purpose of these searches is to fortify its intelligence collage, rather than to accumulate evidence to support indictments and convictions. If the Warrant Clause were held inapplicable here, then the federal intelligence machine would literally enjoy unchecked discretion.").

[82] *See* United States v. Jones, 132 S.Ct. 945, 947, 949, 951 (2012).

[83] *Jones*, 132 S.Ct. at 949 (emphasis added).

[84] *Id.* (quoting Brower v. County of Inyo, 489 U.S. 593, 596 (1989) (quoting *Boyd v. United States*, 116 U.S. 616, 626 (1886); Entick v. Carrington, 95 Eng. Rep. 807 (C.P. 1765).

> he is a trespasser, though he does no damage at all; if he will tread upon his neighbour's ground, he must justify it by law.[85]

A first reading of this opinion might persuade one to think that the Court is reverting back to a pre-1960's Fourth Amendment reading; however, at second glance, Scalia is clear to qualify his reasoning based upon the specific facts[86], and states that the "reasonable expectation of privacy" that may be at issue in this case is unreviewable for lack of preservation.[87] The Majority may have declined to reach as far as other Courts have in the past, however the concurring justices, fearful that this opinion might be misinterpreted, held firmly to the infamous "reasonable expectation of privacy" analysis, first identified by Justice Harlan in his concurring opinion in *Katz v. United States*.

C. *Katz v. United States* explains that a "reasonable expectation of privacy" must exist for there to be a search.

In *Katz*, a wiretap was placed on a payphone that was located in a telephone booth. While it is true that there is no right to privacy in those areas that are public, the Court held that as a man has a right to privacy behind the doors of his own home,[88] he also has a right to privacy

---

[85] United States v. Jones, 132 S.Ct. 945, 949 (2012) (quoting *Brower*, 489 U.S. at 596) (quoting *Boyd*, 116 U.S. at 626; *Entick*, 95 Eng. Rep. at 817) (Internal citation omitted).

[86] *Jones,* 132 S.Ct. at 945. The specific issue referred to in this case only begs the question whether a comparable trespassory Fourth Amendment search occurred when the government installed a GPS on a suspect's car. *Id.* Though the Court did not discuss whether the defendants had a reasonable expectation of privacy, the lower court hinted at this as a problem. *Id.*

[87] *Jones*, 132 S.Ct. at 945.

[88] Weeks v. United States, 232 U.S. 883 (1914).

in those areas that he expects to be private.[89] Jumping over the hurdle that the phone booth is public, the Court analogized his relation to the phone booth as one of a baillee or renter.[90] For the time that he paid his money and shut the door, he owns that space.[91] Though the walls of the booth might be glass, when closed up, the booth becomes private from the rest of the world.[92] Where one walks inside a telephone booth and purposely shuts the door, he is said to believe that his communications will not be overheard by anyone just passing by.[93] This was declared an invasion into his personal space.[94] Expanding upon the holding, Justice Harlan concluded, that communications inside a closed phone booth are an interest that society is ready to protect.[95] Thus declared finding his argument rooted in a "reasonable expectation of privacy" test that Courts later struggled to define.[96]

In *United States v. Karo*, the Supreme Court was asked to decide whether the physical application of a beeper placed on a can of ether, later sold to the suspect and used to track the movements of the cocaine dealers over a period of several months amounted to a search under the Fourth Amendment.[97] This form of tracking did not amount to a search, since the can was

---

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

[90] *Id.*

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] *Katz*, 389 U.S. at 347.

[95] *Id.*

[96] *Katz*, 389 U.S. at 347.

[97] United States v. Karo, 468 U.S. 705, 707 (1984); *see also Cellular Phone Evidence*, *supra* note 10, at 1.

traceable on the open roads and then later kept in a storage locker at commercial storage house.[98] The Court held that the ability of law enforcement to pinpoint a specific storage house in a warehouse lacked the precision to defeat the suspect's expectation of privacy in their own storage locker.[99] Yet, when the can of ether was traced back to a private residence, not open to the public, such warrantless tracking violated the Fourth Amendment.[100]

Smith v. Maryland is another important case that fleshes out "the reasonable expectation of privacy" test.[101] In that case, the Supreme Court held that the use of a pen register was not a search because the defendant lacked any reasonable expectation of privacy in the phone numbers he willingly dialed.[102]

V. The intermediate courts struggle to find common ground.

The Supreme Court has remained silent as to whether the warrantless use of cell-site location data is constitutional, but the Appellate Courts are making some noise. In 2010 a Texas court of appeals decided "whether investigators could compel cellular service carriers to provide cell-site information for targeted phones over a sixty-day period without obtaining a warrant."[103]

---

[98] *Karo*, 468 U.S. at 705.

[99] *Id.* at 708.

[100] *Id.* at 714.

[101] *See* Smith v. Maryland, 442 U.S. 735, 738-40 (1979).

[102] *See id.* at 745-46. Responding to privacy concerns, Congress quickly enacted the Pen Register Statute to protect against police abuses of such location data information.

[103] *See* In re U.S. for Historical Cell-Site Data, 747 F.Supp.2d 827, 846 (S.D. T.X. 2010); *see Cellular Phone Evidence*, *supra* note 10, at 1.

The court acknowledged that "although GPS (satellite) tracking can locate an individual within 10 meters[104] of his location, network (cellular) tracking is more pervasive and practical in criminal investigations, due to the limitations of GPS. Those limitations include the fact that older cell phone models lack the equipment for GPS; GPS works reliably only outdoors, where the handset cell phone has an unobstructed view of several GPS satellites in the sky above and that GPS can be disabled by the cell phone user."[105]

Furthermore, "because the size of a typical cell has been decreasing as more towers are built, and because of Congressional mandates to develop wireless location technology in order to enhance the nation's emergency response system, network tracking is becoming increasingly more precise."[106] Following the guidance of Karo, [107]the court found that sixty days of warrantless cell phone tracking using modern technology was much more intrusive than the *Karo* beepers.[108] For this reason the district court concluded that "court decisions allowing the government to compel cell-site data without a probable cause warrant were based on yesteryear's

[104] Some sources report that GPS can pinpoint a user's location within twenty meters. Smithsonian National Air and Space Museum, *supra* note 48.

[105] *See* In re U.S. for Historical Cell-Site Data, 747 F.Supp.2d 827, 832 (S.D. Tex. 2010); *see also Cellular Phone Evidence*, *supra* note 10, at 1.

[106] *See* In re U.S. for Historical Cell-Site Data, 747 F.Supp.2d 827, 833 (S.D. Tex. 2010); *see Cellular Phone Evidence*, *supra* note 10, at 1.

[107] *See supra* notes 97-100 and accompanying text.

[108] *See* In re U.S. for Historical Cell-Site Data, 747 F.Supp.2d 827, 837 (S.D. Tex. 2010); *see also Cellular Phone Evidence*, *supra* note 10, at 1. The *Karo* court declined to find a search when the beeper located a storage locker but could not pin point the precise location within. *See* Karo, 468 U.S. at 705.

assumption that cell-site data (especially from a single tower) could locate users only imprecisely."[109] Notably, the court denied an application for appeal.[110]

Conversely, in New York, a federal district judge denied a probable cause mandate and accepted the government's hybrid theory combining the standards of both the Stored Communications Act[111] and the Pen Register and Trap and Trace Device,[112] which together, deliver a standard of "relevance and materiality" to a government request for telephone number tracking.[113] In 2010, another court accepted the "relevant and material" argument stating that the Stored Communications Act was vague in reference to what standard would apply, but that the statute itself could be interpreted as not requiring a warrant.[114]

VI. United States v. Jones provides little guidance as it stands.

As recent as 2012, the Supreme Court dodged an analogous "reasonable expectation of privacy" argument when it decided the *United States v. Jones* case. The case discusses the legality of physically installing a GPS device on a suspect's car for the

[109] In re U.S. for Historical Cell-Site Data, 747 F.Supp.2d 827, 837 (S.D. Tex. 2010); *see Cellular Phone Evidence*, *supra* note 10 at 1.

[110] *See* In re U.S. for Historical Cell-Site Data, 747 F.Supp.2d 827, 837 (S.D. Tex. 2010); *see also Cellular Phone Evidence*, *supra* note 10 at 1.

[111] 18 U.S.C. §2703(c)(1)(2009); *see* Wallentine, *supra* note 9, at 404-05 (2011).

[112] Electronic Communications Privacy Act, 18 U.S.C. §§ 3121-3127 (2006); *see* Wallentine, *supra* note 9, at 404.

[113] *See* In re Application of the U.S. for an Order for Disclosure of Telecommunications Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F.Supp.2d 435, 449 (S.D.N.Y. 2005); *see* Wallentine, *supra* note 9, at 404.

[114] David Kravets, *Court Oks Warrantless Cell-Site Tracking*, The Wire.com, (Sept. 7, 2010), http://www.wired.com/threatlevel/2010/09/cell-site-data/.

purposes of tracking that suspect's movements without a warrant.[115] While the majority of the justices found the physical installation of a GPS device to be a search deserving of probable cause, they were split in their reasoning.[116] The majority opinion reasoned that because the Government failed to preserve the argument regarding whether a reasonable expectation of privacy exists in the continuous monitoring of cell-site location tracking, the physical, tangible intrusion of the device installation for the purposes of monitoring was the only issue to be discussed. Thus, this case did not fall under the *Katz* line of reasoning and the decision therefore was founded in Fourth Amendment property rights.[117] As a result, *Jones's* majority opinion provides little guidance.

VII. Conclusion: The Need for Uniformity

The ACLU has brought urgency to the need for uniformity. In September 2011, the ACLU filed an appeal asking the Courts to force the government to turn over information relating to all investigations where cell-site location data was used without a warrant.[118] While this decision has no legal implications on the debate, it demonstrates that civil activists are on the move to ensure that privacy rights remain protected, even if the information is stored and openly available to third parties.

---

[115] United States v. Jones, 132 S.Ct. 945 (2012).

[116] *Id.*

[117] *Id.*

[118] *See generally* Am. Civil Liberties Union v. U.S. Dept. of Justice, 655 F.3d 1 (2011).

In response to the courts' split decisions, a privacy lawyer for the Electronic Frontier Foundation summed up the only workable solution: "What we need at this point is a clear, nationwide standard when it comes to government access to this personal information."[119] The courts, with their hodge-podge of decisions have made it clear that the current statutes that could encompass cell-site location tracking and precedent that somewhat relates to cell-site location tracking are ambiguous at best. Without a new statute that considers the expanding nature of digital surveillance under the cloud of Fourth Amendment privacy, the courts will continue to be divided.

[119] Kravets, *supra* note 114.