ASA

Annie Searle & Associates LLC

**Research Note**

# Cell Site Location Information And Fourth Amendment Protection

Brian Stanley

May 2017



Keywords: Fourth Amendment; Cell Site Location Information; Privacy

*Abstract: This timely paper delves into an in-depth look at implications of government access to and use of cell site location information (CSLI), and the implication for citizens' fourth amendment protection. In 2017, the U.S. Supreme Court will review of Carpenter vs. United States, which argues that CSLI should be protected under the Fourth Amendment.*

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

- "The Constitution of the United States," Amendment 4

Over the past three decades, a period during which wireless telecommunications technology frequently outpaced (and outpaces) Fourth Amendment-based legislation, lower federal and state courts rendered conflicting decisions in the interpretation and application of its protections involving personal wireless cell site location information.

Regarding government's access to and use of non-content communications information, in 2017, U.S. citizens remain uniformly unprotected. Specifically, the Fourth Amendment provides no protection for the majority of U.S. citizens who possess wireless telecommunications devices (cellphones) with respect to their cell site location information (CSLI). Citizens of six U.S. states, based on lower court rulings, have Fourth Amendment protections involving CSLI. Citizens of the remaining forty-four states, based on lower court rulings or no such rulings, have no Fourth Amendment CSLI protections.

In 2017, based on appeal of a Sixth Circuit Court's decision, the U.S. Supreme Court will review Petitioner Timothy Ivory Carpenter's argument (represented by Nathan Freed Wessler) proposing CSLI should be protected under the Fourth Amendment. Ironically, in 2010, the Sixth Circuit Court proclaimed under appeal from the U.S. District Court for the Southern District of Ohio at Cincinnati "…the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."[1]

From a technological standpoint, it is material to the 2017 *Carpenter vs. United States* case, that in 2012 the Justices ruled "the Government's attachment of the GPS device to the vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search (requiring a warrant) under the Fourth Amendment."[2]

Currently, Americans have no uniform protection of their CSLI that is generated by devices, typically, carried on their person twenty-four hours per day. The near-permanence of these personal devices is especially significant given much less time, on average, is spent inside a personal vehicle (for the subset of Americans who possess or use one). While CSLI's accuracy rate is, currently, slightly inferior to that recorded by GPS tracking devices, future FCC mandates must be adopted by U.S. wireless carriers which will result in eventual closure of this (accuracy) difference.

Advances in wireless telecommunications technology, combined with the patchwork of state and lower federal court rulings involving CSLI, necessitates a ruling in favor of U.S. Supreme Court Petitioner Timothy Carpenter's appeal. Rejection of his appeal, in the words of the Sixth Circuit Court unfortunately places the Fourth Amendment at continued risk of obsolescence.

**Fourth Amendment**

The Fourth Amendment to the U.S. Constitution protects the people's right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."

**Third-Party Doctrine**

This doctrine holds "that knowingly revealing information to a third party relinquishes Fourth Amendment protection of said information." While probable cause and a search warrant are required to search one's home, under the third-party doctrine only a subpoena and prior notice (a much lower hurdle than probable cause) are needed to subject, for example, an Internet Service Provider (ISP) to disclose the contents of a customer's email.

In Katz v. United States (1967), the United States Supreme Court "established its reasonable expectation of privacy test." In 1976 (United States v. Miller) and 1979 (Smith v. Maryland), the Court affirmed "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[3]

In Smith v. Maryland (1979), the Court addressed "the question whether the [government's] installation and use of a pen register constitutes a 'search' within the meaning of the Fourth

Amendment." The Court distinguished the use of a pen register from a listening device because pen registers "do not acquire the contents of communications"; they merely acquire the numbers dialed. The Court used this determination to characterize the defendant's argument as a "claim that he had a 'legitimate expectation of privacy' regarding the numbers he dialed on his phone."[4]

**Stored Communications Act (SCA)**

Enacted as Title II of the Electronic Communications Privacy Act (ECPA) of 1986, the "Stored Communications Act (SCA) is a law that addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party ISPs.

The SCA regulates access to stored wire and electronic communications information and transactional records and describes the procedures available to law enforcement agencies to obtain this information under two mutually exclusive categories: "information which contains the contents of communications" or "information which does not contain the contents of communications".[5]

Under the "non-content" communications category, the ECPA mandates a subpoena is sufficient in cases where the (non-content) data contains "specific articulable facts" related to an investigation. In contrast, under the "content" communications category, issuance of a warrant is required once "probable cause" is approved by a court.

While the Fourth Amendment does not define "probable cause", courts over time have established its defining factors: "information sufficient to warrant a prudent person's belief that the wanted individual had committed a crime (for an arrest warrant) or that evidence of a crime or contraband would be found in a search (for a search warrant)".[6]

**U.S. Public Commercial Wireless Telecommunications Services**

Just three years before the SCA's passing, implementation of the first commercial analogue cellular systems (named Advanced Mobile Phone System, AMPS) was successfully completed in the U.S. in select major metropolitan areas, e.g. Chicago.

At its inception, due to the high cost of equipment and service and the lack of ubiquitous coverage, the SCA's ruling affected an infinitesimally small number of Americans. In the three decades since its passage, as shown in Figure 1, the number of Americans possessing cellphones has increased dramatically.

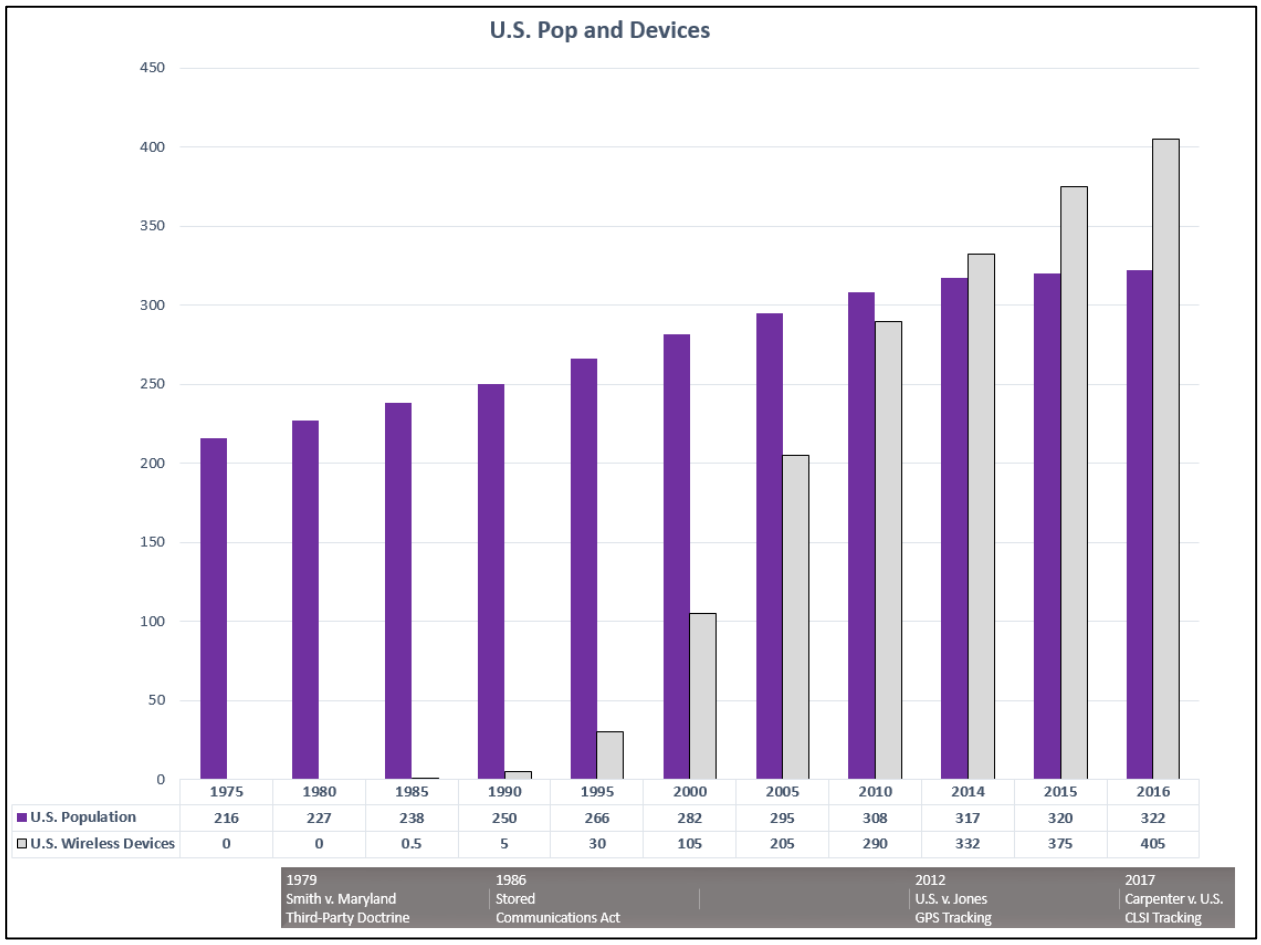


**Figure 1**

While Figure 1 (gray vertical bars) shows the number of U.S. Wireless devices (inequivalent to the number of Americans who own wireless devices), a 2017 Pew survey indicates, "95 percent of Americans own a cellphone" (Figure 2).[7]

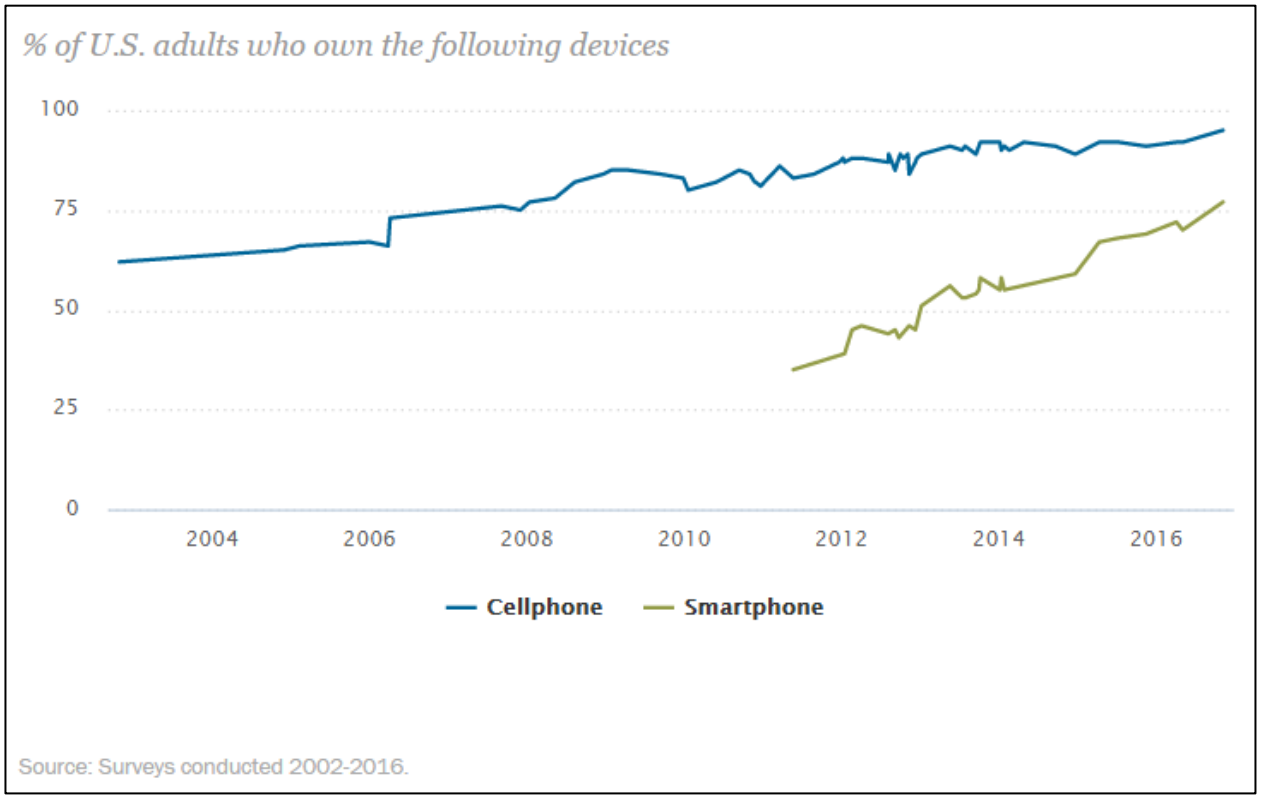


**Figure 2**

Equally notable is the exclusive use of cellphones by a large segment of the population: "As of 2012, cellphones were the only phones used in over one quarter of all American households, a percentage that has nearly tripled in the last five years."[8]

### Cell Site Location Information

Stationary or not, in use or not, the location of a powered-on cellphone is constantly recorded by the wireless carrier serving the device. "Network-based techniques utilize the service provider's network infrastructure to identify the location of the handset. The advantage of network-based techniques (from a mobile operator's point of view) is that they can be implemented non-intrusively, without affecting the handsets. The accuracy of network-based techniques varies, with cell identification as the least accurate and triangulation as moderately accurate, and newer "Forward Link" timing methods as the most accurate. The accuracy of network-based techniques is both dependent on the concentration of base station cells, with urban environments achieving the highest possible accuracy, and the implementation of the most current timing methods."[9]

There are three different means by which a law enforcement agency may compel a wireless

carrier to disclose a subscriber's (current and/or historical) CSLI: the agency may "obtain a warrant or obtain a court order for such disclosure… or get the consent of the subscriber or customer to such disclosure."

Specifically, a "court order for disclosure . . . shall issue only if the governmental entity offers specific articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought are relevant and material to an ongoing criminal investigation."

Therefore, a law enforcement agency's showing of reasonable suspicion is sufficient for a court to grant a governmental entity's order request. The government "is not statutorily required to show probable cause in order to obtain a court order compelling a CSP to disclose a subscriber's records."[10]

**First State Ruling Protecting CSLI**

In 2005, Magistrate Judge Orenstein in the Eastern District of New York was the first judge to deny a government request for CSLI based on his determination it lacked proof of probable cause. In doing so, Judge Orenstein "revealed that the Justice Department had routinely been using a baseless legal argument to get secret authorizations from a number of courts, probably for many years. Many more public denials followed from other judges, sharply rebuking the government and characterizing its legal argument as "contrived," "unsupported," "misleading," "perverse," and even a "Hail Mary" play. Unfortunately, the government succeeds in its reliance of their argument in nearly all other lower federal and state courts."[11]

**State-By-State CSLI Rulings**

As shown in Figure 3, Fourth Amendment protection of CSLI is dependent not on where you reside – it is dependent upon your current and past locations. For example, a Washington State resident, within their home state's border, have zero Fourth Amendment protection – law enforcement may request attainment of CSLI sans warrant.

In contrast, the same Washington State resident traveling in Montana and California (and four other states) is protected under the Fourth Amendment – a warrant is necessary to obtain their CSLI.

In Illinois and Indiana, a warrant is required for real-time CSLI tracking whereas a court order is sufficient to obtain historical CSLI.[12]

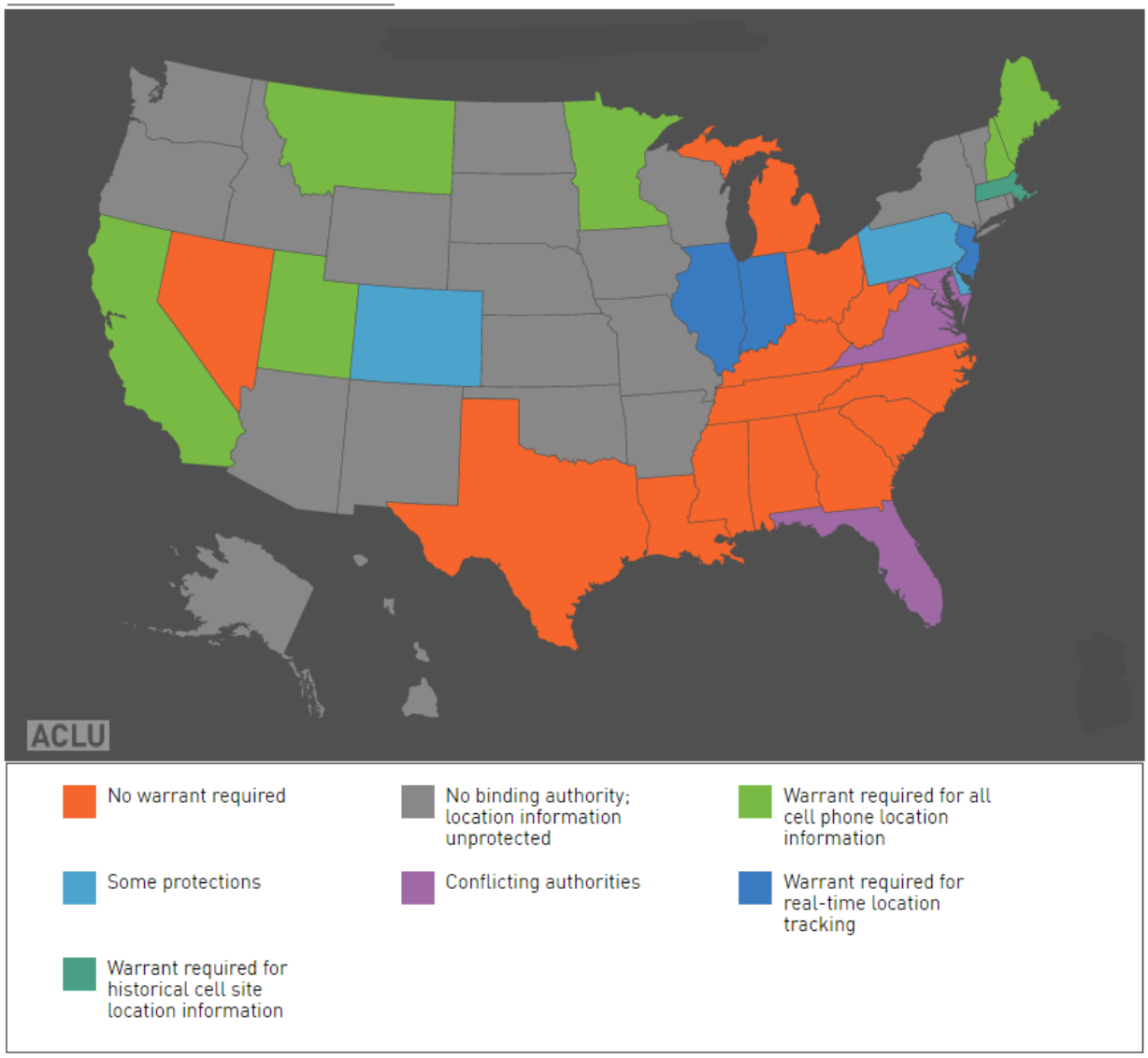


**Figure 3**

### U.S. Wireless Carriers CSLI Information Policies

The four largest U.S. wireless carriers (AT&T, Sprint, T-Mobile, Verizon), which combined serve ninety-nine percent of all U.S. wireless devices,[13] require a warrant when served a CSLI request. This CSLI information policy is documented in each of their "Transparency Reports" which are published (publicly online) semi-annually. Among other metrics, the reports detail the number of CSLI requests submitted, by government and law enforcement agencies, and processed by each wireless carrier.

In 2014, the first-ever "Transparency Report" was published by a wireless carrier. "San Francisco-based CREDO is a progressive organization that supports causes like marriage equality and environmental activism… its wireless service arm is a small part of that, with around 125,000

subscribers."[14]

Transparency Reports were, initially, published by a small number of non-telecom companies including Apple, Facebook, Google, Microsoft, Twitter, and Yahoo. The publications were in response to concerns customers' information was being shared with government agencies without regard to Fourth Amendment protections. In one of the most recent egregious cases of illegal surveillance, beginning in 2001, AT&T conspired with the National Security Agency (NSA) to allow interception of "phone calls and Internet communications." and "receiving wholesale copies of American's telephone and other communications records." (NSA Spying on Americans, 2015)

In 2014, Verizon became the first major wireless carrier to publish Transparency reports detailing CSLI requests. Within the past three years, AT&T, Sprint, and T-Mobile joined Verizon in publishing biannual Transparency Reports. Each carrier, except T-Mobile, provides the specific number of CSLI requests received and processed. Figure 4 shows the total number of CSLI requests annually by carrier. T-Mobile's Transparency Report provides only the total number of warrants received and processed – a superset of requests which include CSLI. For this reason, their data is excluded from Figure 4.

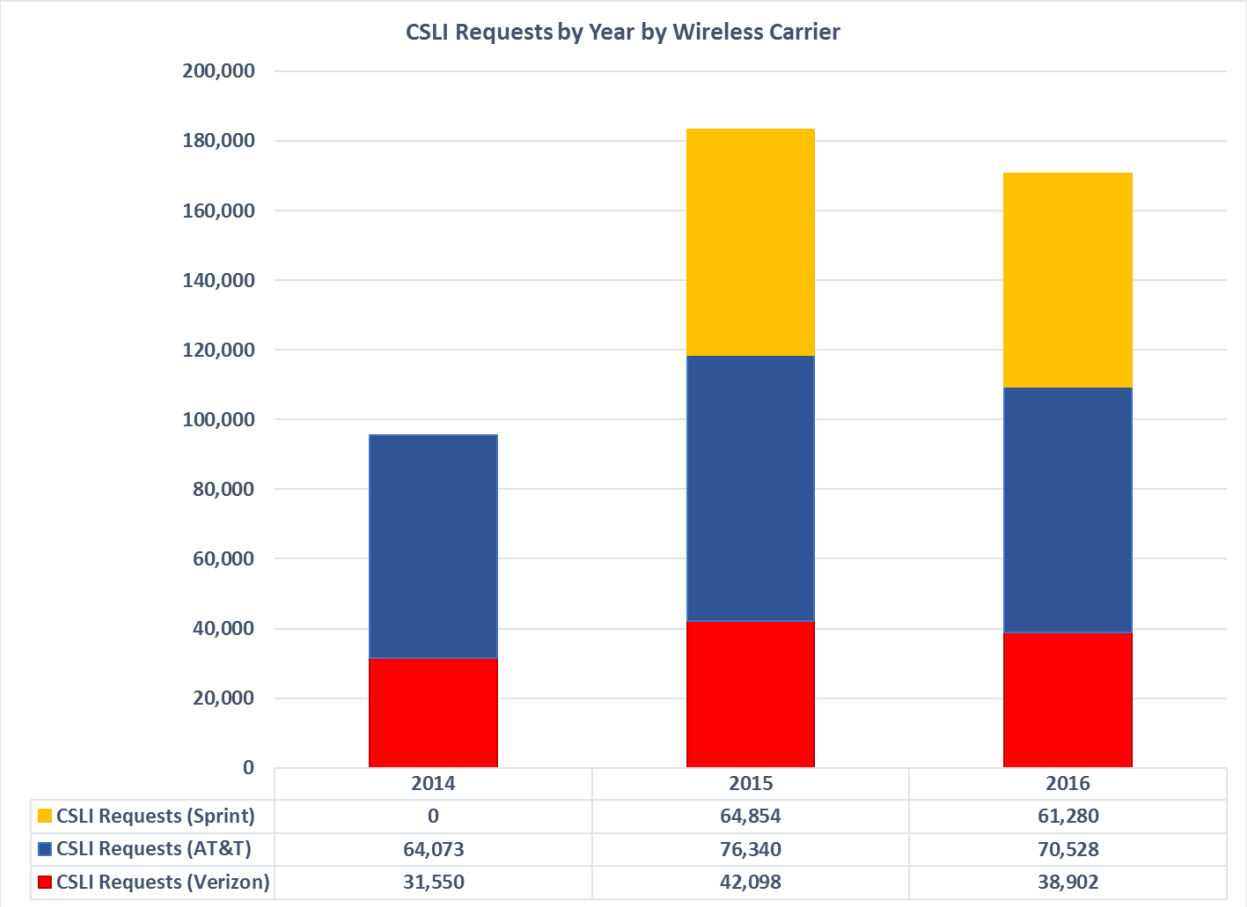


Figure 4

### 2012 U.S. Supreme Court Rules Vehicle GPS Tracking is protected under the Fourth Amendment

In this case, the government obtained a search warrant permitting it to install a Global-Positioning-System (GPS) tracking device on a vehicle registered to a spouse of Jones who was a suspected Washington D.C. narcotics dealer.

The warrant authorized installation of the device only within Washington D.C. and no later than 10 days after its issuance. On the 11th day after issuance of the warrant, law enforcement agents installed the device while the vehicle was parked in the state of Maryland.

Over the subsequent 28 days, the government tracked the vehicle's movements. Following the investigation, an indictment was secured (and, later, a conviction) against Jones (and others) on drug trafficking conspiracy charges. Under the indictment, however, the District Court suppressed the GPS data that was obtained while the vehicle was parked at Jones' residence. Data,

recorded while the vehicle was on public streets, was ruled admissible because Jones had no reasonable expectation of privacy under such conditions.

Ultimately, the D. C. Circuit reversed Jones' conviction, concluding that admission of the evidence obtained by warrantless use of the GPS device violated the Fourth Amendment – due to its installation occurring after the warrant's deadline and outside its jurisdiction.

Under appeal, in United States v. Jones, 2012, the U.S. Supreme Court ruled "The Government's attachment of the GPS device to the vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search (requiring a warrant) under the Fourth Amendment."[15]

**Ubiquity of Wireless Coverage and Wireless Device Use and CSLI Accuracy**

This five-year-old ruling is remarkable given that citizens, currently, have no uniform protection of CSLI that is generated by devices most Americans carry on their person nearly twenty-four hours per day. Time that, on average, is significantly greater than that spent traveling in a personal vehicle (for those who own or use a personal vehicle).

One may argue that CSLI is far less accurate than GPS tracking devices and is therefore unworthy of Fourth Amendment protection. This position, in years past when legacy wireless technology was less sophisticated, was not entirely baseless. Future technological advances and government mandates, however, render the argument groundless.

In 2015, the Federal Communications Commission (FCC) issued its Fourth Report and Order requiring upgrades to its Wireless E911 Location Accuracy Requirements. Specifically, all wireless carriers must provide "(911) dispatchable location or x/y (coordinates) location within 50 meters (164 feet) for the following percentages of wireless 911 calls within the listed timeframes":[16]

- By end of 2017: 40 percent of all wireless 911 calls
- By end of 2018: 50 percent of all wireless 911 calls
- By end of 2020: 70 percent of all wireless 911 calls
- By end of 2021: 80 percent of all wireless 911 calls

Currently, by utilizing sophisticated measurements taken at the time of transmission, CSLI may be determined within 200 feet – a capability which is a five-fold improvement on the FCC's standing requirement that "wireless carriers have the ability to locate ninety-five percent of calls made to or from cellphones accurately within 300 meters (984 feet) or less."

In contrast, "cellphones equipped with GPS can be pinpointed within fifty feet.[17] Figure 5 shows a simplistic example of the differences, on the University of Washington campus, between a 50-foot width (GPS) space (purple rectangular) and a 200-foot width (CSLI) space (blue rectangle). The 200-foot space equals, approximately, one city block whereas the 50-foot space is one-quarter of one city block. In both cases, tracking an individual is relatively non-complex in an urban environment offering standard wireless coverage.

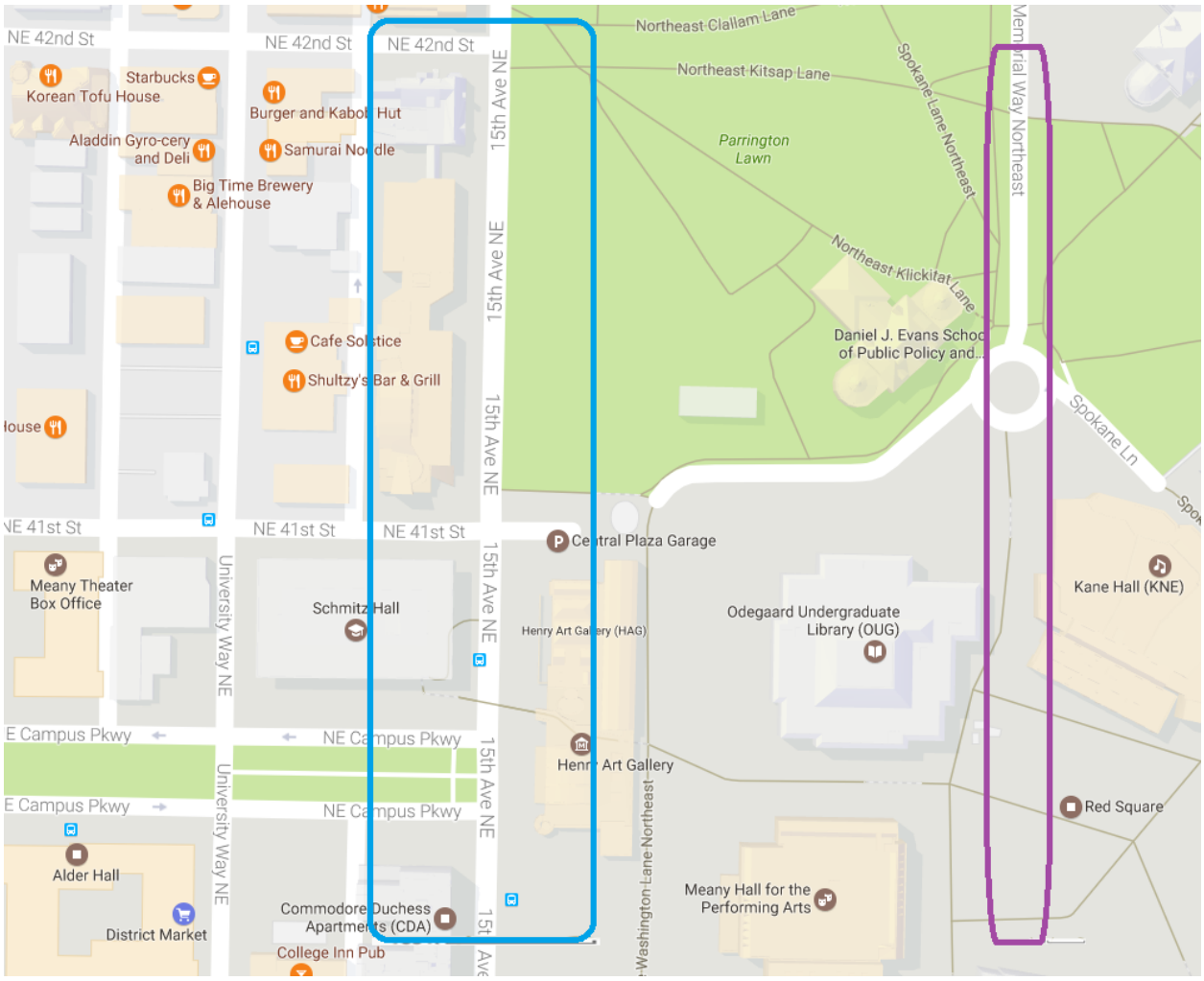


**Figure 5**

In 2008, seven years prior to the FCC's 2015 mandate, Magistrate Judge Lisa Pupo Lenihan of the Western District of Pennsylvania wrote a lengthy denial of an application to compel a cellphone service provider to disclose historical CSLI without a warrant: "As technology now stands... CSLI enables a covert observer to know our physical movements/locations within 50 feet; and our

cellphones… broadcast this information continuously. It is, therefore, extremely difficult to see how a cellphone is not now precisely an electronic... device which permits the tracking of the movement of a person or object. As other courts have observed, tracking device and cellphone technologies have converged."[18]

**Conclusion**

In April 2016, the Sixth Circuit Court of Appeals held, in *Carpenter vs. United States*, that "we lack any privacy interest in the location information generated by our cellphones… a complete disregard for the sensitive and revealing nature of cell site location information and a misguided response to the differences between the analog technologies addressed in old cases and the data-rich technologies of today."[19]

In four separate opinions, eight courts of appeals judges have explained their conclusion that "there is a reasonable expectation of privacy in historical CSLI and that the third-party doctrine does not apply."[20]

The 2012 *United States v. Jones* ruling, combined with the large volume of law enforcement requests for CSLI, conflicting patchwork of laws, significant advances in wireless technology, use of cellphone devices by most American adults, near ubiquitous coverage of wireless services, and future FCC mandates, ought to compel the U.S. Supreme Court to favor Petitioner Timothy Ivory Carpenter's 2017 argument thereby extending Fourth Amendment protection to both historical and real-time CSLI.

---

[1] *United States Court of Appeals for the Sixth Circuit. U.S. v Steven Warshak.* Electronic Frontier Foundation. 14 Dec. 2010. Accessed Mar. 2017 <www.eff.org>.

[2] *United States vs. Jones*. Legal Information Institute, Cornell University Law School. Jan. 23 2012. Accessed Mar. 2017 <www.law.cornell.edu>.

[3] "What You Need To Know About the Third-Party Doctrine." *The Atlantic*. Dec. 2013. Accessed Mar. 2017 <www.theatlantic.com>.

[4] Fox, Christopher. "Checking In: Historic Cell Site Location Information and the Stored Communications Act." *Seton Hall Law Review,* Seton Hall University. 14 May 2012. Accessed Mar. 2017 <www.scholarship.shu.edu>.

[5] Ibid.

[6] "Search and Seizure." The Oxford Index. N.D. Accessed Mar. 2017 <www.oxfordreference.com>.

[7] "Mobile Fact Sheet." Pew Research Center. 12 Jan. 2017. Accessed Mar. 2017 <www.pewinternet.org>.

[8] Fox.

[9] "Cell Phone Tracking." The STADIUM Project, the European Commission. Oct. 2012. Accessed Mar. 2017 <www.largeevents.eu>.

[10] Fox.

[11] "USA v. Pen Register (Cellphone Tracking Cases)." Electronic Freedom Foundation. N.D. Accessed Mar. 2017 <www.eff.org>.

[12] "Cell Phone Location Tracking Laws By State." American Civil Liberties Union. N.D. Accessed Mar. 2017 <www.aclu.org>.

[13] "How Wireless Carriers Stack-Up in Q3 2016." 11 Nov. 2016. Fierce Wireless. Accessed Mar. 2017 <www.fiercewireless.com>.

[14] Fung, Brian. "The First Phone Company to Publish A Transparency Report Isn't AT&T Or Verizon." *The Washington Post.* 9 Jan. 2014. Accessed Mar. 2017 <www.washingtonpost.com>.

[15] *United States vs. Jones.*

[16] "Wireless E911 Location Accuracy Requirements - Fourth Report and Order." Federal Communications Commission. 29 Jan. 2015. Accessed Mar. 2017 <www.fcc.gov>.

[17] Malone, Kyle. "The Fourth Amendment and the Stored Communications Act: Why the Warrantless Gathering of Historical Cell Site Location Information Poses No Threat to Privacy." *Pepperdine Law Review*. 15 Apr. 2012. Accessed Mar. 2017 <www.digitalcommons.pepperdine.edu>.

[18] Lenihan, Lisa Pupo. "Opinion and Memorandum Order: In the Matter of the Application of the U.S.A. for an Order directing a Provider to disclose records to the Government." U.S. District Court for the Western District of Pennsylvania. 19. Feb. 2008. Electronic Freedom Foundation. Accessed Mar. 2017 <www.eff.org>.

[19] Lynch, Jennifer. "Sixth Circuit Disregards Privacy in New Cell Site Location Information Decision." Electronic Freedom Foundation.13 Apr. 2016. Accessed Mar. 2017 <www.eff.org>.

[20] "Reply in Brief in Opposition – *Carpenter vs. United States*." American Civil Liberties Union. Feb. 2017. Accessed Mar. 2017 <www.aclu.org>.