APPELLATE COURT

OF THE

STATE OF CONNECTICUT

A.C. 32803

STATE OF CONNECTICUT

v.

KENDALL O. SMITH, SR.

On Appeal from the Tolland Judicial District
Case. No. T19RCR100096200S
Honorable Stanley T. Fuger Jr.

BRIEF AMICUS CURIAE OF ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT-APPELLANT SMITH

Glenn W. Falk
CT Juris # 102929
NEW HAVEN LEGAL ASSISTANCE ASSOCIATION, INC.
426 State Street
New Haven, CT 06510
Tel. (203) 946-4811
Fax (203) 498-9271
Email: gfalk@nhlegal.org

LOCAL COUNSEL

Hanni M. Fakhoury
CA Bar #252629
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel. (415) 436-9333
Fax (415) 436-9993
Email: hanni@eff.org

LEAD COUNSEL
PRO HAC VICE Pending

STATEMENT OF INTEREST OF AMICUS CURIAE

The Electronic Frontier Foundation (EFF) is a non-profit, member-supported civil liberties organization based in San Francisco, California. EFF has particular expertise concerning law enforcement use of new technologies, including location-based tracking techniques such as GPS and the collection of cell site tracking data. EFF has served as counsel or amicus curiae in federal and state cases throughout the country addressing Fourth Amendment and state constitutional claims in this area. See, e.g., United States v. Jones, 132 S. Ct. 945 (2012); United States v. Katzin, 732 F.3d 187 (3d Cir. 2013); In re Application of the United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); In re Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Record to Gov't, 620 F.3d 304 (3d Cir. 2010); Commonwealth v. Rousseau, 465 Mass. 372, 990 N.E.2d 543 (2013); United States v. Jones, 908 F. Supp. 2d 203 (D.D.C. 2012).

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

State Cases

Federal Statutes

State Statutes

Federal Constitutional Provisions

State Constitutional Provisions

Other Authorities

INTRODUCTION[1]

This case involves an important, disputed[2] question that implicates the privacy of all Connecticut citizens: whether historical cell site location information ("CSLI") – records collected and held by a cell phone company and capable of establishing a person's location, his patterns of movement and ultimately his associations and affiliations – should be protected by the requirements of a search warrant. The answer to this question requires this Court to confront the "power of technology to shrink the realm of guaranteed privacy." Kyllo v. United States, 533 U.S. 27, 34 (2001). Little is more revealing than a person's movements over time. As the D.C. Circuit recently noted, "[r]epeated 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." United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), aff'd sub nom. United States v. Jones, 132 S. Ct. 945 (2012).

The potential for the police to use CSLI to intrude on a constitutionally protected expectation of privacy means this Court should require police seek a search warrant before obtaining CSLI.

---

[1] No one, except for undersigned counsel, has authored the brief in whole or in part, or contributed money towards the preparation of this brief.

[2] Compare In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 559 (D. Md. 2011) (warrant required to obtain prospective GPS and cell site tracking data); In the Matter of an Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 119 (E.D.N.Y. 2011) (warrant required to obtain cell site tracking data) with In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 614 (5th Cir. 2013) (warrant not required); In the Matter of the Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 319 (3d Cir. 2010) (warrant may be required at the discretion of the court).

ARGUMENT[3]

I. Historical CSLI Reveals a Detailed Map of a Person's Location Over Time.

As courts encounter evolving technologies, they must reject "mechanical interpretation[s] of the Fourth Amendment." Kyllo, 533 U.S. at 35-36. "The meaning of a Fourth Amendment search must change to keep pace with the march of science." United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007) (citing Katz v. United States, 389 U.S. 347 (1967) and Kyllo, 533 U.S. at 34). There is no question that technology advances have allowed CSLI to become a powerful tool capable of revealing an enormous amount of detail about a person's movements and locations.

A cell phone is a two-way radio that connects to a cellular network by sending radio signals to a nearby "cell site." See generally In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 750-52 (S.D. Tex. 2005).[4] A "cell site" consists of a cell phone tower, a radio transceiver and a base station controller. Id. at 750. The three directional antennas in a cell site divide the site into a number of "sectors" to handle communications to the cellular network.[5] When a cell phone is on, it "announces its presence to a cell tower via a radio signal." Id. at 751. This process is known as "registration" or "identification." Id.

---

[3] To be clear, in large part this case hinges on whether the so-called "third party doctrine" – the idea that an individual has no expectation of privacy in information disclosed to third parties – applies to historical cell site information. See Smith v. Maryland, 442 U.S. 735, 743–44 (1979). For the sake of brevity, EFF agrees with the arguments made by amicus the Connecticut Criminal Defense Lawyers Association contesting this idea.

[4] See also Testimony of Matt Blaze, Associate Professor, University of Pennsylvania, House Committee on the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security Hearing on ECPA, Part 2: Geolocation Privacy and Surveillance, April 25, 2013.

[5] Thomas A. O'Malley, Using Historical Cell Site Analysis Evidence in Criminal Trials 59 U.S. Attorneys' Bull. Nov. 2011, at 16, 19, available at http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf.

Cell phones are now ubiquitous in the United States. CTIA, the wireless cell phone trade association, reported that by December 2012, there were 326.4 million cell phones in the United States, meaning cell phones outnumber the population of the United States.[6] Earlier this year, the Pew Research Center reported that for the first time, a majority of American adults – 56% – owned Internet-enabled "smartphones" such as the Apple iPhone or Google's line of "Android" phones.[7] Smartphones are essentially miniature computers, allowing a user to check their email, access websites and even communicate with others over the phone's built in video camera.

Naturally, these Internet tasks have resulted in a significant increase in the amount of wireless data traffic being handled by cell sites. CTIA reported the amount of wireless data increased by 278% between 2010 and 2012.[8] The use of more data means there are more frequent connections to cell sites. This is particularly true with Internet enabled smartphones. In order to receive and download emails or perform other network functions, smartphone programs – known as applications or "apps" – remain running even when a user has the phone tucked away in their pocket or purse, and thus smartphones communicate with cell sites much more frequently than traditional cell phones.[9]

---

[6] CTIA - The Wireless Association, Wireless Quick Facts: Year-End Figures, available at http://www.ctia.org/advocacy/research/index.cfm/aid/10323.

[7] Aaron Smith, Smartphone Ownership — 2013 Update, at 2, Pew Research Center, *available at* http://pewinternet.org/~/media//Files/Reports/2013/PIP_Smartphone_adoption_2013_PDF.pdf.

[8] CTIA - The Wireless Association, Semi-Annual Wireless Industry Survey: Reported Wireless Data Traffic, available at http://files.ctia.org/pdf/CTIA_Survey_YE_2012_Graphics-FINAL.pdf.

[9] See Gyan Ranjan, et al., Are Call Detail Records Biased for Sampling Human Mobility?, 16 Mobile Computing & Comm. Rev. 3, 34 (2012), available at http://www-users.cs.umn.edu/~granjan/Reports/MC2R_2012_CDR_Bias_Mobility.pdf ("Unlike voice-calls and SMS activities, (user) data activities do not always require user initiation, nor user participation. For example, a plethora of applications running on 3G enabled cellular

Most importantly for this Court, the growing demand for cell phones and smartphones has resulted in an explosion in the number of cell sites across the country. In the last ten years, CTIA reported an 85% increase in the number of cell sites in the United States.[10] In December 2007, a month before the ex parte order at issue here, CTIA reported there were approximately 213,299 cell sites in the United States. But by the end of 2012, there were 301,779 cell sites in the United States, a 29% increase in just five years.

In addition to faster connection speeds, this expansion in cell sites also means that a person's location can be pinpointed with greater precision. See In the Matter of an Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d at 534 ("Due to advances in technology and the proliferation of cellular infrastructure, cell-site location data can place a particular cellular telephone within a range approaching the accuracy of GPS."). The accuracy of cell site data depends on the size of the sector. A sparsely populated rural area may only have one cell site servicing a wide geographical area. But a dense urban area would need many sectors and cell sites, each serving a smaller geographical area. The smaller the geographical area, the greater the ability to pinpoint a person's location accurately.

For example, a searchable database of publicly available cell tower and antenna information reveals there are approximately 656 antennas and 108 cell phone towers within a four mile radius of the Connecticut Appellate Court at 75 Elm Street in Hartford,

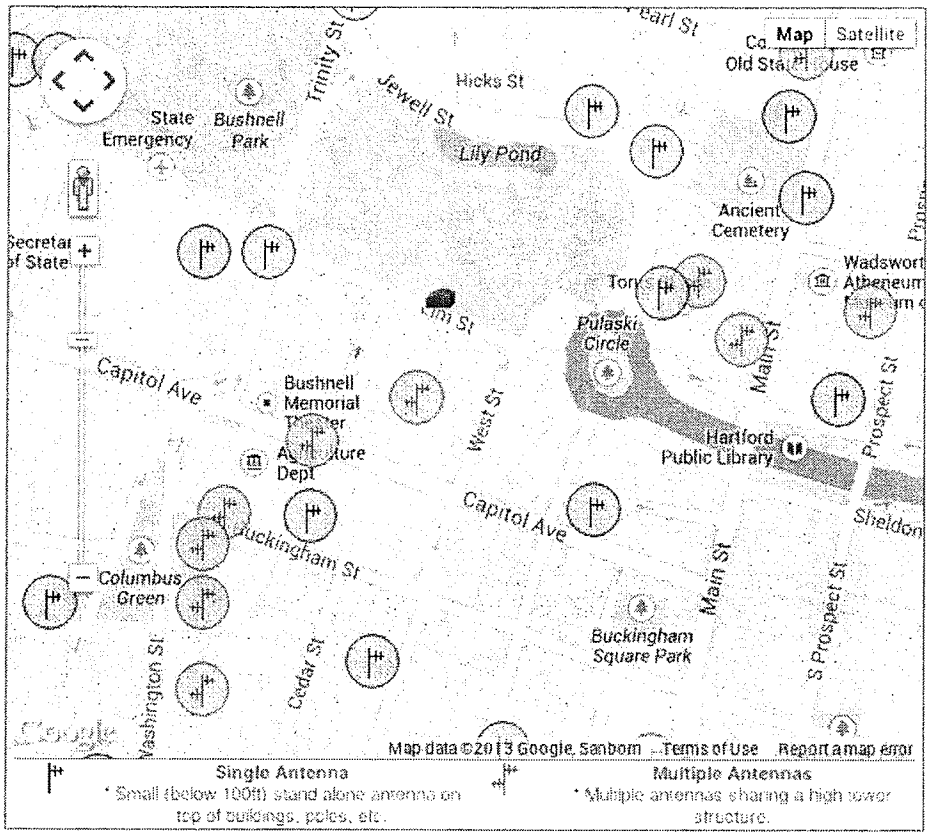
---

devices invoke themselves periodically or sporadically. These include push-mail notifications, periodic software updates and weather services, to name a few.").

[10] CTIA - The Wireless Association, Semi-Annual Wireless Industry Survey: Commercially-Operational Cell Sites in the U.S., available at http://files.ctia.org/pdf/CTIA_Survey_YE_2012_Graphics-FINAL.pdf.

Connecticut.[11] In this dense urban area, knowing which tower or antenna a phone connected to would reveal on which side of Trinity Street a person was closest to when they made a call or received an email, or, if a person was standing on Capitol Avenue when sending a text message, whether they were closer to West or Main Street.

- **Antenna Sites - (75 Elm St, Hartford, CT 06106)**



Law enforcement wants access to CSLI because of its accuracy and precision in pinpointing an individual near the scene of a crime. For example, in United States v. Skinner, 690 F.3d 772 (6th Cir. 2012), law enforcement was able to track a phone (and the person carrying it) almost 770 miles from Tucson, Arizona to Abilene, Texas over two days.

[11] General Data Resources, AntennaSearch.Com, Search conducted on September 20, 2013, available at http://www.antennasearch.com/sitestart.asp?sourcepagename=reportviewer2&prevsessionidnum=214624746&prevordernum=1&previtemnum=1&sectionname=txreview&pagename=txreview&pagenum=1&cmdrequest=pagehandler.

Skinner, 690 F.3d at 776.[12] Agents could see the suspect's travel point by point, and waited until he stopped at a rest stop before swooping in to arrest him. Id. Most critically, "[a]t no point did agents follow the vehicle or conduct any type of visual surveillance." Id. The cell phone made the government surveillance easier. Agents would not need to follow the truck physically around the clock or run the risk that they would be discovered. Nor did they need to find a way to surreptitiously install a GPS device onto the truck to track its movements. Instead, as the New Jersey Supreme Court recently noted, cell site information "is akin to using a tracking device and can function as a substitute for 24/7 surveillance without police having to confront the limits of their resources." State v. Earls, 214 N.J. 564, 586, 70 A.3d 630, 642 (2013).

The monitoring that occurred here – obtaining six months worth of phone records detailing Smith's location – is far more invasive than the tracking in Skinner. Last year U.S. Supreme Court Justice Sotomayor cautioned that long-term location 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." Jones, 132 S. Ct. at 955 (Sotomayor, J., concurring). And cell phone tracking can even reveal information about a person in the most constitutionally protected space: a home. One federal magistrate judge has noted "pinging a particular cellular telephone will in many instances place the user within a home, or even a particular room of a home." In the Matter of an Application of U.S. for an Order Authorizing Disclosure, 849 F. Supp. 2d at 540; see also In re Application of U.S. for an Order for Prospective Cell Site Location Info. on a

[12] Skinner involved real time location tracking as opposed to historical location information. Both reveal an enormous amount of sensitive information about where a person goes and whom they associate with. Arguably, historical location information leads to an even more intrusive government action: the recreation of a person's past movements.

Certain Cellular Tel., 460 F. Supp. 2d 448, 462 (S.D.N.Y. 2006) (warning government's use of cell site data to "surveil a target in a private home that could not be observed from public spaces" could be unconstitutional).

This is not just a hypothetical concern. Earlier this year, a team of researchers from Harvard and MIT determined that it took just a minimal amount of location information gathered from anonymized cell phone location information to uniquely identify 95% of the users.[13] That is, armed with 15 months worth of anonymized mobile phone data of 1.5 million users, researchers could identify a specific individual with merely four sets of hourly updates of which cell phone tower a person connected to. As the authors note, "the uniqueness of human mobility traces is high" and yet a cell phone makes this information easily accessible to the government.[14]

Given the sensitive details CSLI reveals, it is clear that it must be safeguarded by requiring law enforcement obtain a search warrant before accessing this information.

II. Since People Have a Reasonable Expectation of Privacy in their Location, the Fourth Amendment and Article First, § 7 Require Police Obtain a Search Warrant to Acquire Historical CSLI.

Both the Fourth Amendment to the United States Constitution and article first, § 7 of the Connecticut Constitution prohibit "unreasonable" searches and seizures. A "search" occurs when the government violates a "reasonable expectation of privacy." Jones, 132 S. Ct. at 949-50. The "reasonable expectation of privacy" test is defined as an "actual

---

[13] See Yves-Alexandre de Montjoye, et al., Unique in the Crowd: The privacy bounds of human mobility, Scientific Reports, March 25, 2013, available at http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html; see also Kim Zetter, Anonymized Phone Location Data Not So Anonymous, Researchers Find, Wired, March 27, 2013, *available at* http://www.wired.com/threatlevel/2013/03/anonymous-phone-location-data/.

[14] Yves-Alexandre de Montjoye, supra note 13.

(subjective) expectation of privacy" that "society is prepared to recognize as 'reasonable.'" Katz, 389 U.S. at 361 (Harlan, J., concurring); see also State v. Joyce, 229 Conn. 10, 20, 639 A.2d 1007, 1013 (1994) (Katz formulation of "reasonable expectation of privacy" applies to article first, § 7). This Court has made clear, however, that article first, § 7 may provide stronger privacy protection beyond that provided in the Fourth Amendment. State v. Legrand, 129 Conn. App. 239, 257, 20 A.3d 52, 65 (2011); State v. Jenkins, 298 Conn. 209, 261, 3 A.3d 806, 840 (2010). Under both the Fourth Amendment and article first, § 7 people have an expectation of privacy in their location that requires police obtain a warrant before tracking movements for an extended period of time.

The United States Supreme Court most recently addressed expectations of location privacy in Jones. Federal agents installed a GPS device without a search warrant underneath the car of a suspected drug dealer. Jones, 132 S. Ct. at 948. Agents tracked Jones' public movements for 28 days throughout the District of Columbia and Maryland. Id. Ultimately, Jones was arrested and convicted of conspiracy to distribute drugs, and sentenced to life in prison. Id. at 948-49. Defending the search on appeal before the D.C. Circuit, the government argued that United States v. Knotts, 460 U.S. 276 (1983) held that a person had no reasonable expectation of privacy in movements he exposed to the public while driving on public streets. Maynard, 615 F.3d at 556.

The D.C. Circuit rejected this argument, noting that Knotts did not contemplate the prolonged visual surveillance enabled by a GPS device. Id. Knotts was concerned with "movements during a discrete journey." Id. (citing Knotts, 460 U.S. at 283). Aggregating those movements, however, "reveals more – sometimes a great deal more – than does the sum of its parts," including "what a person does repeatedly, what he does not do, and what

he does ensemble." Maynard, 615 F.3d at 558, 562. The key inquiry, then, was not whether another person can possibly discover the information, but whether a person *reasonably expects* that another person might actually discover the information. Id. at 559. While portions of a person's daily travels are often exposed to some people, pervasive and invasive surveillance has an entirely different character. The "whole of one's movements over the course of a month is not actually exposed to the public because the likelihood anyone will observe all those movements is effectively nil." Id. at 558. The result was thus an "unknown type of intrusion into an ordinarily and hitherto private enclave." Id. at 565.

The Supreme Court affirmed the D.C. Circuit on different grounds, finding the warrantless trespass onto Jones' property for the purpose of obtaining information for a criminal investigation constituted a "search" under the Fourth Amendment. Jones, 132 S. Ct. at 954. Yet, all members of the Supreme Court noted the possibility that electronic monitoring of a person's location could violate a reasonable expectation of privacy. Justice Scalia's majority opinion stated "mere visual observation does not constitute a search," but cautioned it "may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy." Id. at 953-54. But the majority felt it did not need to conclusively decide the issue. Id. at 954.

In concurring opinions by Justices Sotomayor and Alito, a majority of the Justices echoed the D.C. Circuit's concern with the capabilities of technology to cheaply and efficiently aggregate reams of data to create new and unknown intrusions into previously private places. See id. at 956 (Sotomayor, J., concurring) and 963 (Alito, J., concurring in the judgment). To Justice Sotomayor, technology advances that make "available at a relatively low cost such a substantial quantum of intimate information about any person" to

the state "may alter the relationship between citizen and government in a way that is inimical to democratic society." Id. at 956 (Sotomayor, J., concurring) (citations and quotations omitted). The fact that the state could obtain similar information through "lawful conventional surveillance techniques" rather than new technologies was not "dispositive" of the Fourth Amendment issue. Id.; see also Kyllo, 533 U.S. at 35, n.2 ("The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment.").

On location privacy specifically, both concurring opinions in Jones found that "longer term GPS monitoring . . . impinges on expectations of privacy." Jones, 132 S. Ct. at 964 (Alito, J., concurring in the judgment); id. at 955 (Sotomayor, J., concurring). Justice Sotomayor questioned "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the state to ascertain . . . their political and religious beliefs, sexual habits, and so on." Id. at 956 (Sotomayor, J., concurring). Justice Alito believed "society's expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual's car for a very long period." Id. at 964 (Alito, J., concurring in the judgment).

Both before and after Jones, other courts looking at GPS surveillance under the Katz expectation of privacy test have determined that prolonged GPS surveillance is a "search" under the Fourth Amendment. See State v. Zahn, 812 N.W.2d 490, 496 (S.D. 2012) (use of GPS to track a car for 26 days was a "search" under Katz); United States v. Lopez, 895 F. Supp. 2d 592, 602 (D. Del. 2012) (defendant had "reasonable expectation that the vehicles he was using would not be tracked by electronic surveillance" for 17 days). Numerous state courts have also found GPS surveillance to be a "search" under their state constitutions.

See, e.g., Commonwealth v. Rousseau, 465 Mass. 372, 990 N.E.2d 543 (2013) (relying on Jones concurring opinions to find GPS surveillance a "search" under state constitution); People v. Weaver, 12 N.Y.3d 433, 909 N.E.2d 1195 (2009); State v. Campbell, 306 Or. 157, 759 P.2d 1040 (1988); State v. Jackson, 150 Wash. 2d 251, 76 P.3d 217 (2003).

While the cases mentioned above all involve GPS surveillance, they are still applicable to the constitutionality of acquiring cell site location information. Ultimately, Maynard and the concurring opinions in Jones demonstrate that regardless of *how* electronic surveillance is conducted, people nonetheless maintain a reasonable expectation of privacy in their aggregated movements – even their public movements – since society would deem it unlikely that anything more than small, discrete movements would be observed at a time. That means individuals also have a reasonable expectation of privacy to be free from surveillance pieced together through historical CSLI, triggering the requirement of a search warrant supported by probable cause and judicial oversight.

The New Jersey Supreme Court recently applied the concurring opinions in Jones to historical CSLI in Earls. There, police acquired cellphone tower data from T-Mobile without a search warrant. Earls, 214 N.J. at 570, 70 A.3d at 633-34. Reviewing under New Jersey's state constitution, the court found the warrantless acquisition unconstitutional. Id. at 570, 70 A.3d at 633. Critically, as highlighted in Maynard and Justice Alito's concurring opinion in Jones, the New Jersey high court believed cell site tracking involved "a degree of intrusion that a reasonable person would not anticipate." Id. at 586, 70 A.3d at 642 (citing Jones, 132 S. Ct. at 964 (Alito, J., concurring in judgment)). Ultimately, CSLI reveals a "broad range of personal ties with family, friends, political groups, health care providers, and

others," details which "provide an intimate picture of one's daily life." Earls, 214 N.J. at 586, 70 A.3d at 642 (citing Jones, 132 S. Ct. at 955-56 (Sotomayor, J., concurring)).

This Court should reach the same conclusion as Earls. No matter the technology, tracking a person's movement triggers an expectation of privacy, requiring a search warrant.

III. A Search Warrant Requirement Will Not Create An Unnecessary Burden on Police.

Imposing a search warrant requirement would not result in an unnecessary burden on law enforcement because the law currently requires the government seek judicial authorization before obtaining CSLI.

Under Conn. Gen. Stat. § 55-47aa(b), a judge may order the release of phone records if law enforcement "states a reasonable and articulable suspicion that a crime has been or is being committed." This standard for disclosure is similar to that in the federal Stored Communications Act ("SCA") which requires the government demonstrate to the court "specific and articulable facts showing that there are reasonable grounds to believe . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).[15] Since both Connecticut and federal law requires law enforcement to necessarily seek judicial authorization before obtaining CSLI from a cell phone provider, there is little procedural difference between the process currently in place and that for obtaining a search warrant. Both involve ex parte

[15] The SCA permits states to impose more stringent access requirements on state law enforcement officials. See 18 U.S.C. § 2703(d) ("[i]n the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State."). But even when it comes to federal law enforcement officers, the Third Circuit has ruled that the SCA gives judges discretion to require a search warrant in some instances before agents can obtain historical CSLI. In re Application of U.S. for an Order, 620 F.3d at 319 (§ 2703 gives court "the option to require a warrant showing probable cause."); but see In re Application of U.S. for Historical Cell Site Data, 724 F.3d at 607-08 (disagreeing with the Third Circuit).

proceedings before a judge, who hears the facts known to law enforcement by way of affidavit and affirmation to determine whether the appropriate legal standard has been met.

A search warrant requirement would only make two changes to the current procedure. First, it would change the legal standard that must be met before the state can access these records. Instead of showing "reasonable and articulable suspicion" under Connecticut law, or demonstrating the records are "relevant and material" as required by federal law, the state would have to convince the judge there was "probable cause" instead. That means a court would have to find the state had proven there was a "fair probability that contraband or evidence of a crime will be found in a particular place." State v. Sivri, 231 Conn. 115, 142, 646 A.2d 169, 183 (1994) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

Second, the judge would have greater authority to supervise the execution of a search warrant. The Supreme Court has explained, "responsible officials, including judicial officials, must take care to assure that [searches] are conducted in a manner that minimizes unwarranted intrusions upon privacy." Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976). When it comes to electronic surveillance in particular, warrants typically have "minimization" requirements that limit electronic surveillance to ensure "similar protections to those that are present in the use of conventional warrants authorizing the seizure of tangible evidence." Berger v. New York, 388 U.S. 41, 57 (1967); see also In re Appeal of Application for Search Warrant, 2012 VT 102, ¶ 28, 71 A.3d 1158, 1170 (Vt. 2012), cert. denied, 133 S. Ct. 2391 (2013). And with search warrants, officers are required to return to the court within ten days of execution with an inventory of what they seized. See, e.g., Conn. General Statutes § 54-33c(a) ("The warrant shall be executed within ten days and

returned with reasonable promptness . . . and shall be accompanied by a written inventory of all property seized.").

Yet these minor differences between an order issued under state and federal law and a search warrant are constitutionally significant. While they impose only a minimal additional burden upon law enforcement, they play an important role in limiting police searches and safeguarding privacy. The probable cause standard "protects 'citizens from rash and unreasonable interferences with privacy and from unfounded charges of crime.'" Maryland v. Pringle, 540 U.S. 366, 370 (2003) (quoting Brinegar v. United States, 338 U.S. 160, 176 (1949)). Judicial supervision over the warrant process is important too, as "the Fourth Amendment has interposed a magistrate between the citizen and the police . . . so that an objective mind might weigh the need to invade that privacy in order to enforce the law." McDonald v. United States, 335 U.S. 451, 455 (1948); see also Gates, 462 U.S. at 240 ("essential protection" of warrant requirement is for evidentiary inferences to "be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.") (quotations omitted).

Even the return requirements are arguably constitutionally significant, ensuring that discretion as to what is to be seized is not determined solely by the officer. See Berger, 388 U.S. at 60 ("Nor does the statute provide for a return on the warrant thereby leaving full discretion in the officer as to the use of seized conversations"); Wayne R. LaFave, 2 Search & Seizure § 4.12(c) (5th ed.) ("it is not fanciful to suggest that the requirement of a return inheres in the Fourth Amendment"); see also Commonwealth v. Ocasio, 434 Mass. 1, 5, 746 N.E.2d 469, 473 (2001) (search warrant return requirement allows defendant to raise challenges to state's collection of evidence).

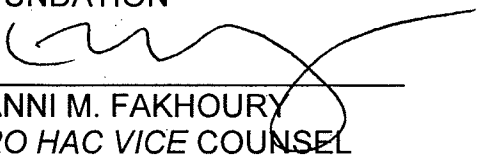
When it comes to new surveillance technology, judicial oversight is especially important to ensure the invasive capabilities of new technologies do not "alter the relationship between citizen and government in a way that is inimical to democratic society." Jones, 132 S. Ct. at 956 (Sotomayor, J., concurring)). Long term electronic surveillance poses the serious risk of upsetting the traditional relationship between citizen and state by avoiding what has long been the "greatest protection[] of privacy:" "practical" restraints such as the cost and difficulty of maintaining long-term, covert surveillance. Jones, 132 S. Ct. at 963 (Alito, J., concurring in judgment). Since cell site surveillance, like GPS monitoring, "is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" Id. at 956 (Sotomayor, J., concurring) (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)). Judicial oversight must provide this crucial check on law enforcement as technology eradicates the more traditional restrictions on police power.

CONCLUSION

Historical CSLI is a valuable crime-fighting tool because of its power to intrude on a traditionally private sphere to obtain an enormous amount of sensitive information about where a person has been, their patterns of movements and their associations and affiliations. Law enforcement should be permitted to use this information to keep people safe, provided they adhere to strict safeguards designed to protect privacy. The proper way to balance these interests is to require a search warrant supported by probable cause before authorizing disclosure of cell site location information. The lower court's decision should be reversed.

Respectfully submitted,

ELECTRONIC FRONTIER FOUNDATION



HANNI M. FAKHOURY
PRO HAC VICE COUNSEL
(Application Pending)
California Bar No. 252629
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
Fax (415) 436-9993
hanni@eff.org

GLENN W. FALK
LOCAL COUNSEL
Juris No. 102929
New Haven Legal Assistance Assn., Inc.
426 State Street
New Haven, CT 06510-2018
(203) 946-4811
Fax (203) 498-9271
gfalk@nhlegal.org

CERTIFICATION OF SERVICE AND FORMAT

This is to certify that a copy of the foregoing amicus curiae brief was mailed, first-class postage prepaid, this ____ day of December, 2013, to The Honorable Stanley T. Fuger, Jr., Superior Court, G.A. 12, 410 Center Street, Manchester, CT 06040; Pamela S. Nagy, P.O. Box 12607, Philadelphia, PA 19129, (205) 842-3162, Fax (215) 842-1813, pam.nagy@comcast.net; Marjorie A. Dauster, Office of the Chief State's Attorney, 300 Corporate Place, Rocky Hill, CT 06067, (860) 258-5807, Fax (860) 258-5858, marjorie.dauster@ct.gov; Paul Bailin, Shipman & Goodwin LLP, One Constitution Plaza, Hartford, CT 06103, (860) 251-5011, Fax (860) 251-5099, pbailin@goodwin.com; and Moira Buckley, Law Office of Moira Buckley, LLC, 55 Oak Street, Suite 4, Hartford, CT 06106, (860) 724-1325, Fax (860) 724-1326, mbuckley@mbuckleylaw.com.

This is also to certify that the application complies with all the provisions of Practice Book §§ 67-2 and 67-7.

_____

Glenn W. Falk