IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	)
	)
v.	) No. 05-CR-386(1) (ESH)
	)
ANTOINE JONES,	)
	)
Defendant.	)

_____)

BRIEF *AMICI CURIAE* OF THE ELECTRONIC FRONTIER FOUNDATION AND CENTER FOR DEMOCRACY & TECHNOLOGY IN SUPPORT OF DEFENDANT ANTOINE JONES' MOTION TO SUPPRESS CELL SITE DATA

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Constitutional Provisions

Legislative Materials

Other Authorities

STATEMENT OF *AMICI CURIAE*

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported organization based in San Francisco, California, that works to protect free speech and privacy rights in an age of increasingly sophisticated technology. As part of that mission, EFF has served as counsel or *amicus curiae* in many cases addressing civil liberties issues raised by emerging technologies, including location-based tracking techniques such as GPS and collection of cell site tracking data.

The Center for Democracy & Technology ("CDT") is a non-profit public interest organization focused on privacy and other civil liberties issues affecting the Internet, other communications networks, and associated technologies. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

INTRODUCTION

Earlier this year, the Supreme Court ruled that the government's installation of a GPS tracking device on a motor vehicle to track Antoine Jones' location over a prolonged period of time constituted a Fourth Amendment search. *United States v. Jones*, 132 S. Ct. 945 (2012). On remand, Jones now moves to suppress data obtained from his cell phone provider — without a warrant — that the government acquired to monitor Jones' location over six months.

Specifically, the government invoked 18 U.S.C. §§ 3122, 2123, and 2703(d) to obtain from Jones' cellular phone provider "the location of cell site/sector (physical address) at call origination (for outgoing calls), call termination (for incoming calls), and if reasonably available, during the progress of a call" for a cellular phone number believed to be associated with Jones. Def. Mot. Amend Mot. Suppress Ex. 1 ¶ 11, Ex. 2 ¶ 11, Ex. 3 ¶ 11 (Dkt. No. 609). Initially, the

government sought this data for a 60-day period — twice as long as the GPS data at issue before the Supreme Court was collected. The government subsequently filed two extensions seeking to collect data for a total of approximately six months. As the applications make clear, the government gathered this information for the purpose of tracking Jones' movements during this period. Def. Mot. Amend Mot. Suppress Ex. 1 ¶ 10, Ex. 2 ¶ 10, Ex. 3 ¶ 10.

The motion to suppress must be granted because the government must obtain a warrant based on probable cause to track Jones' location for six months, and the lesser legal standard the government relies upon does not pass constitutional muster.

ARGUMENT

I. THE GOVERNMENT MUST OBTAIN A WARRANT BASED ON PROBABLE CAUSE TO COLLECT SIX MONTHS OF CELL SITE DATA FOR THE PURPOSE OF TRACKING AN INDIVIDUAL'S LOCATION.

Cell phones have become ubiquitous. As one court has noted:

> The vast majority of Americans own cell phones. Many Americans have abandoned land line phones entirely, and use cell phones for all telephonic communications. Typically people carry these phones at all times: at work, in the car, during travel, and at home. For many Americans, there is no time in the day when they are more than a few feet away from their cell phones.

In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 114-15 (E.D.N.Y. 2011).

Jones' motion to suppress should be granted because the government violated the Fourth Amendment when it sought six months' worth of location information from Jones' provider of this essential service without obtaining a warrant based on probable cause.

A. A Person Has a Reasonable Expectation of Privacy in Not Having His Location Tracked By the Government Continuously for Six Months.

The Fourth Amendment protects people against unreasonable government searches and seizures. U.S. Const. amend. IV. A "search" may occur when the government physically

trespasses on personal property in "an attempt to find something or obtain information," *Jones*, 132 S. Ct. at 951 n.5, or when it intrudes upon a person's reasonable expectation of privacy. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *Kyllo v. United States*, 533 U.S. 27, 33 (2001).

In *Jones*, all nine Justices recognized the possibility that electronic monitoring without any physical trespass can violate the Fourth Amendment under the reasonable expectation of privacy test. As Justice Scalia wrote in the majority opinion, joined by Chief Justice Roberts and Justices Sotomayor, Thomas, and Kennedy, "mere visual surveillance does not constitute a search," but "[i]t may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy," although "the present case does not require us to answer that question." *Id.* at 953-54.

In a separate concurring opinion, Justice Sotomayor specifically underscored the fact that prior Supreme Court precedent leaves open the possibility that GPS tracking without a physical trespass may constitute a Fourth Amendment search, but also found it unnecessary to reach the question. *Id.* at 956-57 (Sotomayor, J., concurring) (citing *United States v. Knotts*, 460 U.S. 276 (1983), and *United States v. Karo*, 468 U.S. 705 (1984)).

Justice Alito's concurrence, joined by Justices Ginsburg, Breyer, and Kagan, firmly concluded that prolonged GPS tracking alone — distinct and separate from any trespass — intrudes upon an individual's reasonable expectation of privacy, and therefore is a Fourth Amendment search. *Id.* at 964 (Alito, J., concurring).[1]

[1] Both concurring opinions expressly cited cell phones and data disclosed by individuals to their cell providers as issues of Fourth Amendment concern. *Id.* at 957 (Sotomayor, J., concurring); *Id.* at 963 (Alito, J., concurring).

The government will likely argue that cell cite tracking is not as accurate as GPS data. In fact, cell site information can be quite precise, and the technology is trending in directions that make it increasingly more so. *See In re Application of the U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, No. 10–2188–SKG, 2011 WL 3423370, at *3-5 (D. Md. Aug. 3, 2011) (unpublished) (comparing the precision and tracking capabilities of GPS and cell cite data).

However, precision of certain data elements is not the test for Fourth Amendment purposes. The test is whether the government's actions intruded upon a reasonable expectation of privacy. Individuals have a reasonable expectation that the government will not use electronic surveillance methods to track their locations persistently over a prolonged period of time. Recognizing this, several courts have required probable cause warrants for collection of cell site tracking data over periods far shorter than the six months at issue here.[2]

The collection of cell site tracking information to monitor a person's location over an extended period is distinctly more invasive and revealing than mere visual surveillance. *In the*

---

[2] *See, e.g., In re Application of the U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 2011 WL 3423370, at *3-5 (warrant required to obtain 30 days of GPS and cell site tracking data); *In re Application of the U.S. for an Order Authorizing Release of Historical Cell-Site Info.,* 736 F. Supp. 2d 578, 578-79 (E.D.N.Y. 2010) (warrant required for 58 days of cell site tracking data); *In re Application of the U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827, 829 (S.D. Tex. 2010) (warrant required for 60 days of cell site tracking data); *In re Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, No. 06 Crim. Misc. 01, 2006 WL 468300, at *2 (S.D.N.Y. Feb. 28, 2006) (unpublished) (same); *see also, In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011) (warrant required for 113 days of cell site tracking data). Conversely, some courts have held that no warrant is necessary where the government seeks records for a relatively short period of time. *See, e.g., In re Application of the United States for an Order Authorizing Release of Historical Cell-Site Info.*, No. 11-MC-0113, 2011 WL 679925, at *1 (E.D.N.Y. Feb. 16, 2011) (unpublished) (government permitted to access 21 days of cell site tracking data upon a showing of specific and articulable facts).

Matter of an Application of the U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 2011 WL 3423370, at *9. As the D.C. Circuit explained in *United States v. Maynard*:

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

615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd sub nom. Jones*, 132 S. Ct. 945. Constant location monitoring over a prolonged period enables the government to "generate[] 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 954 (Sotomayor, J., concurring).

B. Cell Site Tracking Data Can Be Used to Situate a Person Within the Home

Tracking one's location through cell site data can reveal information about a person in the space that enjoys the greatest constitutional protection: a private home. In *Karo*, the Supreme Court held that warrantless surveillance with a tracking device violates the Fourth Amendment when it reveals details about an individual's location within a space where he enjoys a reasonable expectation of privacy. 468 U.S. 705, 715-16. One judge considering collection of cell site tracking data has speculated that the government could run afoul of this precedent by using cell site information to "surveil a target in a private home that could not be observed from

public spaces." *In re Application of U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d 448, 462 (S.D.N.Y. 2006). Similarly, a magistrate judge has noted that "pinging a particular cellular telephone will in many instances place the user within a home, or even a particular room of a home, and thus, the requested location data falls squarely within the protected precinct[.]" *In the Matter of an Application of the U.S. for an Order Authorizing Disclosure of Location Information of a Specified Wireless Tel.*, 2011 WL 3423370, at *9-10. As these courts have determined, cell site tracking data may be sufficient to allow government investigators to conclude — and for prosecutors to argue that a jury can conclude — that an individual was in a particular private space at a particular time.

That is exactly what happened in this case. One of the government's rationales for obtaining cell site information here was to "discover[] the location of the *premises* in which the trafficker maintains his supply of narcotics, paraphernalia used in narcotics trafficking such as cutting and packaging materials, and other evidence of illegal narcotics trafficking, including records and financial information." Def. Mot. Amend Mot. Suppress Ex. 1 ¶ 10, Ex. 2 ¶ 10, Ex. 3 ¶ 10 (emphasis added). Under *Karo*, the government's use of information to locate a person in a space in which there is a reasonable expectation of privacy is a "search."

C. The Third-Party Doctrine Does Not Defeat a Person's Reasonable Expectation of Privacy in Not Being Tracked By the Government.

To defeat the Fourth Amendment protection in cell site tracking information, the government has often turned to the so-called "third-party doctrine," or the idea that a person has no legitimate expectation of privacy in information he *voluntarily* conveys to a third party. *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). As many courts have commented, however, users do not "voluntarily" convey their location information to the cell phone provider. *See In re 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, 317-18 (3d Cir. 2010). Moreover, there is growing recognition that the third-party doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (citing *Smith*, 442 U.S. at 742 and *United States v. Miller*, 425 U.S. 435, 443 (1976)).

1. The Third-Party Doctrine Does Not Control Because Users Do Not Voluntarily Convey Their Locations to Cell Providers.

Integral to the third-party doctrine is the idea that a person *voluntarily* relinquishes information and thus loses his expectation of privacy in it. But as many courts have suggested in the context of cell site tracking, users do not truly convey their location to their cell phone provider *voluntarily*. Users do not enter their location into the phone the way they dial the number of the party they are calling. They do not take any affirmative action to create the location information at all. In fact, their location is generated automatically, often without their intent, knowledge, or control. *In re Application for Pen Register & Trap/Trace Device With Cell Site Location Auth.*, 396 F. Supp. 2d 747, 756-57 (S.D. Tex. 2005); *In the Matter of an Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 736 F. Supp. 2d at 582-84; *In the Matter of an Application of the U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 2011 WL 3423370, at *9 n.6.

In the past, the government has argued that cell site tracking records are similar to the records in *Smith v. Maryland*, *supra*. *See, e.g., In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d at 317; *In re U.S. for Historical Cell Site Data*, 747 F. Supp. 2d at 841. In *Smith*, the Supreme Court held that using a pen register to determine the telephone number dialed by an individual was not a Fourth Amendment search. 442 U.S. at 739, 742. The Court relied heavily on the notion that this

information was voluntarily conveyed to the phone company and thus was "exposed" the same way it would have been in the past had the caller told the information to a switchboard operator. *Id.* at 744.

Similarly, in *Miller*, the Supreme Court's ruling that a bank customer had no expectation of privacy in financial records was based on the finding that the records "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." 425 U.S. at 442. Thus in *Smith* and *Miller*, the disclosure of information was constitutional because the transfer involved "affirmative, voluntary steps that a person knows will cause a phone company, or a bank, to learn of it." *Commonwealth v. Pitt*, No. 2010–0061, 2012 WL 927095, at *4 (Mass. Super. Feb. 23, 2012). By contrast, "the average cell phone user is not even aware that use of his cell phone creates a record of his location, much les that such use causes this information to be conveyed to the cell phone company." *Id.*

Cell site tracking is not affirmatively and voluntarily conveyed to the provider in the same way. Rather, it is transmitted "automatically" and "entirely independent of the user's input, control, or knowledge." *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 756-57. It is "neither tangible nor visible to a cell phone user" and when a user "turns on the phone and makes a call, she is not required to enter her own zip code, area code, or other location identifier. None of the digits pressed reveal her own location. Cell site data is generated automatically by the network, conveyed to the provider not by human hands, but by invisible radio signal." *In re Application of U.S. for Historical Cell Site Data*, 747 F. Supp. 2d at 844.

Because this information is transmitted automatically by the phone itself, rather than by anything the user manually does, "a cell phone customer has not 'voluntarily' shared his location

information with a cellular provider in any meaningful way" because "when a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all." *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d at 317-18 (brackets omitted) (internal quotation marks omitted); *see also Pitt*, 2012 WL 927095, at *4 ("[T]he average cell phone user is not even aware that use of his cell phone creates a record of his location, much less that such use causes this information to be conveyed to the cell phone company.").

And without the user "voluntarily" conveying this information to the provider, the third-party doctrine cannot defeat Jones' reasonable expectation of privacy in his location and movements over an extended period of time. The Fourth Amendment applies to this data notwithstanding the third-party doctrine.

2. The Third-Party Doctrine is Poorly Suited to Justify the Collection of Cell Site Tracking Information.

With increasing public awareness of how cell phones work, the number of users who understand the automatic transmission of cell site tracking data will increase. But regardless of whether users understand how their cell phones work or not, "the bare possibility of disclosure by a third party cannot by itself dispel all expectation of privacy." *In re Application of U.S. for Historical Cell Site Data*, 747 F. Supp. 2d at 845.

With an eye to the future, Justice Sotomayor in her concurring opinion in this very case suggested that the third-party doctrine should be reconsidered:

> This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their

> cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice Alito notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year.

Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring). More importantly — channeling Justice Marshall's dissenting opinion in *Smith* — she explained that it is time to end the third-party doctrine's reliance on "secrecy as a prerequisite for privacy." *Id.* She noted that not "all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." *Id.* (citing *Smith*, 442 U.S. at 749 (Marshall, J., dissenting)). As Justice Marshall wrote in *Smith*: "Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes." *Smith*, 442 U.S. at 749 (Marshall, J., dissenting).

This idea — that privacy is not lost simply because some discrete amount of data is turned over to someone else for a limited purpose — is found consistently throughout Fourth Amendment jurisprudence. After all, the phone conversation recorded in *Katz* went through the phone companies' telephone wires, which could be wiretapped, but was nonetheless protected by the Fourth Amendment. 389 U.S. at 353. Similarly, sealed letters and packages passing through the hands of the post office maintain Fourth Amendment protection, despite the ease with which the government could open and inspect them. *See United States v. Jacobsen*, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy."); *Ex parte Jackson*, 96 U.S. 727, 733 (1877).

More recently, *United States v. Warshak* extended Fourth Amendment protection to the contents of email, despite the fact they are always given to third-party providers like Yahoo! or Gmail who store messages and route them to their intended destination. 631 F.3d 266, 288 (6th Cir. 2010). Noting that hotel guests have an expectation of privacy in their rooms even though a maid may enter to clean them, and that tenants have an expectation of privacy in their rented apartments, the Sixth Circuit concluded that "the mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy." *Id.* at 286-87 (citing *United States v. Allen*, 106 F.3d 695, 699 (6th Cir.1997) (hotel rooms) and *United States v. Washington*, 573 F.3d 279, 284 (6th Cir. 2009) (tenants)) (emphasis in original).

The same is true of cell site tracking information. The fact that users disclose their locations to their cell phone providers for proper routing of calls does not defeat their reasonable expectation of privacy in the entirety of their movements over a prolonged period. If a hotel guest does not lose his reasonable expectation of privacy in his personal effects by allowing a housekeeper to enter his room to clean, and a user does not give her email provider free rein to pore over the contents of messages sent or received on the Internet, so too a cell phone user should not lose his right of locational privacy simply because he turned his cell phone on or received a phone call. Allowing such a mundane act — walking around with a cell phone turned on in a pocket or purse — to defeat a reasonable expectation of privacy would allow Fourth Amendment guarantees to founder in the wake of technology.[3]

[3] One judge has proposed an exception to the third-party doctrine specifically for cell site location information. *In re Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d at 125.

II. FEDERAL COMMUNICATIONS LAWS DO NOT AUTHORIZE PROSPECTIVE COLLECTION OF CELL SITE TRACKING DATA ABSENT A PROBABLE CAUSE WARRANT.

In the absence of a search warrant application, the government's request for prospective cell site tracking information in this case hinged on a so-called "hybrid" theory to piece together three related, yet distinct, federal communications statutes: the Pen Register and Trap and Trace Device Statute ("Pen/Trap statute"), 18 U.S.C. §§ 3121, *et seq.*; the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"), 47 U.S.C. §§ 1001, *et seq.*; and the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701, *et seq.* As a Magistrate Judge of this Court has held, the government's creative efforts to construct this hybrid theory fail to justify collection of prospective cell site tracking data without a probable cause warrant. *In re Application of U.S. for an Order Authorizing the Release of Prospective Cell Site Info.*, 407 F. Supp. 2d 134, 139 (D.D.C. 2006) (Facciola, M.J.).

A. Statutory Background.

1. The Pen/Trap Statute and CALEA.

Under the Pen/Trap statute, the government may apply for an order authorizing the installation of a "pen register" or "trap and trace device" if "the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency." 18 U.S.C. § 3122(b)(2). The term "pen register" is defined as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted" and excludes content. 18 U.S.C. § 3127(3). The term "trap and trace device" means "a device or process which captures the incoming electronic or other impulses which identify the originating number or

other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. § 3127(4).

Cell site tracking information constitutes "signaling information" under the Pen/Trap statute. *See United States Telecomm. Ass'n v. FCC*, 227 F.3d 450, 463-64 (D.C. Cir. 2000) ("[A] mobile phone sends signals to the nearest cell site at the start and end of a call. These signals, which are necessary to achieve communications between the caller and the party he or she is calling, clearly are 'signaling information.'") (internal quotations omitted). Consequently, one might think that cell site tracking information could be obtained through an application for the installation of a pen register or trap and trace device.

The government's ability to use a pen register application to obtain cell site tracking information is limited, however, by CALEA. Specifically, 47 U.S.C. § 1002(a) explains "information acquired *solely* pursuant to the authority for pen registers and trap and trace devices. . . shall not include any information that may disclose the physical location of the subscriber." 47 U.S.C. § 1002(a) (emphasis added). Since cell site tracking information discloses the user's "physical location," the Pen/Trap statute does not allow the government to obtain this information.

2. The SCA.

CALEA's use of the word "solely" has caused a considerable amount of debate and judicial disagreement. The government has argued it means that Congress authorized combining the Pen/Trap statute with another statute in order to obtain prospective cell site tracking information. As one court has described the government's theory, CALEA "affirmatively authorizes access to information disclosing the physical location of the subscriber so long as the government does not act 'solely pursuant' to the Pen/Trap Statute." *In re Application of U.S. for*

Orders Authorizing Installation & Use of Pen Registers & Caller Identification Devices on Tel. Numbers [Sealed] and [Sealed], 416 F. Supp. 2d 390, 394 (D. Md. 2006).

The government claims this additional statutory authority is found in the SCA, specifically, 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d). Under 18 U.S.C. § 2703(c)(1)(B), the government is permitted to obtain "a record or other information pertaining to a subscriber to or customer of" an "electronic communication service" if it follows the procedures set forth in 18 U.S.C. § 2703(d).[4] In turn, 18 U.S.C. § 2703(d) authorizes a court to order the disclosure of these records if the government has demonstrated "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

Under the government's interpretation of these statutes, to obtain cell site tracking information it may apply for a "hybrid" order under both 18 U.S.C. § 3122 and 18 U.S.C. § 2703(d). But a number of magistrate and district judges — including Magistrate Judge Facciola of this Court — have held the hybrid theory is insufficient to permit the disclosure of these records.[5] Other courts have disagreed, finding the hybrid theory sufficient to obtain this

---

[4] "Electronic communication service" is defined as a "service which provides to users thereof the ability to send or receive wire or electronic communications," and thus includes cell phone providers. 18 U.S.C. § 2510(15).

[5] *See, e.g., In re Application of U.S. for an Order Authorizing the Release of Prospective Cell Site Info.*, 407 F. Supp. 2d at 140; *In re Application of U.S. for an Order: (1) Authorizing Use of a Pen Register & Trap & Trace Device, (2) Authorizing Release of Subscriber & Other Info., (3) Authorizing Disclosure of Location-Based Services*, 727 F. Supp. 2d 571, 575 (W.D. Tex. 2010); *In re Application of U.S. for Order*, 497 F. Supp. 2d 301, 305-06 (D.P.R. 2007); *In re Application U.S. for Orders Authorizing Installation & Use of Pen Registers & Caller Identification Devices on Tel. Numbers [Sealed] and [Sealed]*, 416 F. Supp. 2d at 394; *In re Application of U.S. for an Order Authorizing Installation & Use of a Pen Register & a Caller*

information.[6] This Court should continue to reject the hybrid theory as an incorrect interpretation of the law.

B. The Hybrid Theory Does Not Authorize Disclosure of Prospective Cell Tracking Information.

As one court has commented, "[i]mplicit in the government's hybrid theory of statutory authority is the acknowledgment that neither the Pen Register Statute nor the SCA standing alone authorizes disclosure to the government of cell site information." *In the Matter of the Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register Device, a Trap & Trace Device, and for Geographic Location Info.*, 497 F. Supp. 2d 301, 305 (D. Puerto Rico 2007). As explained above, the Pen/Trap statute is limited by CALEA and cannot be used as independent authority to obtain a user's physical location. *See* 47 U.S.C. § 1002(a)(2). Nor does the SCA by itself permit the government to obtain prospective cell site tracking information from a cell phone provider. Moreover, using CALEA to attempt to bridge the Pen/Trap statute and the SCA contravenes underlying legislative history. This "hybrid" theory cannot authorize the disclosure of this information.

Identification Sys. on Tel. Numbers (Sealed), *In re U.S. for an Order Authorizing Installation & Use of a Pen Register*, 415 F. Supp. 2d 211, 215 (W.D.N.Y. 2006); *In re Application of U.S. For an Order Authorizing the Disclosure of Prospective Cell Site Info.*, 412 F. Supp. 2d 947, 957 (E.D. Wis. 2006); *In re Application of U.S. for an Order Authorizing Installation & Use of a Pen Register & a Caller Identification Sys. on Tel. Numbers (Sealed)*, 402 F. Supp. 2d 597, 600 (D. Md. 2005); *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 765; *In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device*, 396 F. Supp. 2d at 321; *see also In re Application of U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 2006 WL 468300, at *2.

[6] *See In re Application of U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d at 461; *In Matter of Application of U.S. for an Order,* 411 F. Supp. 2d 678, 680 (W.D. La. 2006); *In re Application of U.S. for an Order for Disclosure of Telecommunications Records & Authorizing the Use of a Pen Register & Trap & Trace*, 405 F. Supp. 2d 435, 448 (S.D.N.Y. 2005).

1. The SCA Provides No Authority for Prospective Location Tracking.

Interpreting the SCA to authorize real time, prospective tracking of individuals through their cell phones stretches the SCA far beyond its original, intended purpose, namely authorizing the government to "compel disclosure of existing communications and transaction records in the hands of third party service providers." *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 760.

The SCA's plain text contemplates only the disclosure of records *already in existence*. First, 18 U.S.C. § 2703(c)(1) authorizes disclosure of "a record or other information" about a user. "Record," by definition, means historical documents already in existence. *See* Merriam-Webster's Collegiate Dictionary, Eleventh Edition, 2010 (defining "record" as "something that recalls or relates *past* events") (emphasis added).[7] While "other information" can mean any number of things, when read in the SCA's context as a whole it is clear that this phrase was intended to ensure that any historical, preserved information pertaining to a subscriber would be protected from disclosure without the need for courts and litigants to quibble over what "record" means.

Second, under 18 U.S.C. § 2703(d), the government can obtain "records" only by demonstrating they "are relevant and material to an ongoing criminal investigation." The "exclusive use of the present tense — rather than, for example, the phrase 'are or may be' — suggests that the items requested must already be in existence." *In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device*, 396 F. Supp. 2d at 313.

[7] http://www.merriam-webster.com/dictionary/record (last accessed August 6, 2012).

This plain reading of the statute is underscored by the legislative history's repeated reference to "records" being "maintained," "kept," or "stored." *See, e.g.*, S. Rep. No. 99-541, 99th Cong., 2d Sess., at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3557; H.R. Rep. 99-647, 99th Cong., 2d Sess., at 25, 72, 73 (1986). One sponsor of the bill, Rep. Robert W. Kastenmeier, emphasized to Congress that one of the "fundamental principles" guiding the legislation is that "the nature of modern recordkeeping requires that some level of privacy protection be extended to records about us which are stored outside the home." *See* 132 Cong. Rec. H4039-01, 1986 776505, at *23-24 (1986).

There is another, more practical reason why the SCA cannot be interpreted to authorize real-time, prospective cell site tracking: it contains none of the provisions found in other statutes authorizing prospective data collection. *See In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 760. For example, the Wiretap Act and Pen/Trap statute both permit a court to order a service provider to give whatever "information, facilities or technical assistance," including the physical installation of hardware or other electronic devices, necessary to perform surveillance. *See, e.g.,* 18 U.S.C. §§ 2511(2)(a)(ii), 3123(b)(2), and 3124. The SCA, in contrast, does not permit a court to issue such an order, authorizing only "disclosure" of requested records. 18 U.S.C. § 2703(d).

Moreover, unlike other prospective surveillance statutes, the "SCA imposes no limit on the duration of the government's access, no provision for renewal of the court order, no requirement for periodic reports to the court by the government, and no automatic sealing of court records." *In re Application of U.S. for Orders Authorizing Installation & Use of Pen Registers & Caller Identification Devices on Tel. Numbers [Sealed] and [Sealed]*, 416 F. Supp. 2d at 395. Congress' decision not to include these provisions in the SCA highlights that the SCA

was not intended to authorize prospective surveillance. *In re Application of U.S. for Order*, 497 F. Supp. 2d at 309.

2. CALEA Was Not Intended to Authorize Prospective Location Tracking.

CALEA makes clear that the government may not use pen register and trap and trace applications to determine a person's physical location. 47 U.S.C. § 1002(a)(2). And the legislative history only confirms CALEA was never intended to authorize prospective cell tracking. The House Judiciary Committee's report on CALEA stated it "[e]xpressly provides that the authority for pen registers and trap and trace devices cannot be used to obtain tracking or location information, other than that which can be determined from the phone number." H.R. Rep. No. 103-827(I), 103rd Cong., 2nd Sess. at 17 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3497.

Moreover, at the time Congress considered CALEA, FBI Director Louis Freeh testified before the House and Senate that the information communication providers would have to turn over to law enforcement was not to include "any information which might disclose the general location of a mobile facility or service beyond that associated with the area code or exchange of the facility or service." Statement of Louis J. Freeh, Director Federal Bureau of Investigation Before the Subcommittee on Technology and the Law of the Committee on the Judiciary, United States Senate, 1994 WL 223962, at *25 (March 18, 1994). In no uncertain terms, he explained that "there is no intent whatsoever. . . to acquire anything that could properly be called 'tracking information.'" *Id.*

In sum, through passage of CALEA, "Congress was discouraging, not encouraging, reliance on the Pen/Trap Statute" for purposes of prospective cell tracking." *In re Application of U.S. for Orders Authorizing Installation & Use of Pen Registers & Caller Identification Devices*

on Tel. Numbers [Sealed] and [Sealed], 416 F. Supp. 2d at 395. Stretching CALEA to somehow confer authority for the government to prospectively track an individual's location contravenes the statute's plain text and its legislative history.

CONCLUSION

This Court must determine the circumstances under which the government may obtain prospective cell site tracking information. Because this information captures constitutionally protected information — a person's location — the government needs a search warrant, supported by probable cause, to obtain it. Neither the Pen/Trap statute nor the SCA authorizes prospective cell phone tracking, and CALEA does not bridge the gap between the two. Thus, the government is required to obtain a warrant to collect prospective cell site tracking information. This Court should grant the motion to suppress.

August 13, 2012

Respectfully submitted,

/s/ Marcia Hofmann

MARCIA HOFMANN
D.C. Bar No. 484136
HANNI FAKHOURY
JON B. EISENBERG
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
Tel: (415) 436-9333
Fax: (415) 436-9993
marcia@eff.org

Counsel for *Amici Curiae*