

UNITED STATES DISTRICT COURT  
DISTRICT OF CONNECTICUT

UNITED STATES OF AMERICA	:	
	:	
vs.	:	CRIMINAL NO. 3:09CR200(AWT)
	:	
LUIS SOTO	:	June 18, 2010

**MEMORANDUM OF *AMICI CURIAE* IN SUPPORT OF MOTION TO SUPPRESS**

The American Civil Liberties Union, ACLU of Connecticut, and Electronic Frontier Foundation respectfully submit this memorandum in support of defendant Luis Soto’s motion to suppress cell site location information that the government obtained without a warrant based on probable cause and particular description, Docket No. 99. The Fourth Amendment requires the government to comply with the warrant requirement before accessing people’s location and movement information, which reveal intimate details of their lives protected by reasonable expectations of privacy.<sup>1</sup>

---

<sup>1</sup> *Amici* confine their memorandum to constitutional arguments that are the source of the suppression remedy. *Amici*’s position on the governing statutory scheme, which does not provide a suppression remedy, *see* 18 U.S.C. § 2708; *United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008), is detailed in their *amici curiae* brief submitted to the Third Circuit. Briefly, *Amici* take the position that historical cell site location information is protected by the SCA because it is a “record . . . pertaining to a subscriber” under the plain language of the statute, regardless of whether a cell phone may be a “tracking device” under the Mobile Tracking Device Act, 18 U.S.C. § 3117. *See* Brief of *Amici Curiae* Electronic Frontier Foundation, the American Civil Liberties Union, the ACLU-Foundation of Pennsylvania, Inc., and the Center for Democracy and Technology in Support of Affirmance of the District Court, In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government at 2-3, No. 08-4227 (3d Cir. Filed March 16, 2009), *available at* <http://www.aclu.org/files/assets/FiledCellTrackingBrief.pdf>.

## BACKGROUND<sup>2</sup>

### I. CELL SITE LOCATION INFORMATION

The “cell site location information,” or “cell site data,” that is at issue in this suppression motion, is location data that is automatically generated by every cell phone in order to connect calls. Whenever a cellular phone is turned on, it scans for a cell tower and the sector of that tower that provides the best reception and, approximately every seven seconds, registers this information with the network.<sup>3</sup> The cell phone carriers keep track of the registration information in order to identify the cell tower through which calls can be made and received.<sup>4</sup>

Cell site location information refers to the identity of the cellular tower from which a cell phone is receiving the strongest signal at the time and the sector of the tower facing the phone.<sup>5</sup> Because the location of the cell tower is known, this information indicates the location of the cell

---

<sup>2</sup> *Amici* have limited access to materials relevant to the defendant’s motion, as many of the materials, such as the order granting access to cell site location information, appear to be under seal. The factual background is therefore based on the defendant’s memorandum in support of motion to suppress and other publicly available materials.

<sup>3</sup> See *In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 534 F. Supp. 2d 585, 589-90 (W.D. Pa. 2008) (Lenihan), *aff’d*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *appeal docketed*, No. 08-4227. For ease of reference, after the first full citation subsequent citations to opinions on cell phone location applications will be referred to by the district court, year, and the judge issuing the opinion.

<sup>4</sup> See *id.*

<sup>5</sup> See, e.g., *In the Matter of the Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Information*, 412 F. Supp. 2d 947, 948-49 (E.D. Wis. 2006) (Callahan), *aff’d*, No. 06-MISC-004, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006) (Adelman).

phone. The information is available both prospectively, to track the phone in real-time,<sup>6</sup> and historically, to retrace previous movements.<sup>7</sup>

## II. § 2703(D) ORDER

According to Soto's suppression memorandum, law enforcement officers in this case obtained historical cell site location information for all incoming and outgoing calls from 180 target numbers, including Soto's. Mem. in Support of Mot. to Suppress ("Mem.") at 1, 3, Docket No. 100. They obtained this information pursuant to an order issued under 18 U.S.C. § 2703(d) of the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq.* ("a D order"), on a showing that the information is "relevant and material to an ongoing investigation." They did not obtain a warrant or show probable cause.

The government's actions in this case are consistent with some prosecutors' practice of applying for a D order to obtain historical cell site location information. In a number of these instances, like this one, it appears that the applications are unchallenged and remain under seal. In one of the few published decisions regarding government access to historical cell site location information, however, the Western District of Pennsylvania—with all magistrate judges signing the opinion—held that the government must obtain a warrant to access this information, in part

---

<sup>6</sup> See, e.g., *In the Matter of the Application of the United States of America for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking*, 441 F. Supp. 2d 816, 817 (S.D. Tex. 2006) (Smith).

<sup>7</sup> See, e.g., *W.D. Pa. 2008 (Lenihan)*, 534 F. Supp. 2d at 586 n.4.

because such applications raise constitutional concerns.<sup>8</sup> That decision, which was affirmed by the district court,<sup>9</sup> is now on appeal in the Third Circuit.

### III. GOVERNMENT'S PLANNED USE OF CELL SITE LOCATION INFORMATION AS EVIDENCE

According to the defendant's memorandum, the government intends to use the cell site location information that it obtained to "map the approximate locations and movements of the defendant's telephone and those of four other people that the government believes were involved in the bank robbery of the Webster Bank on July 25, 2008." Mem. at 1-2. "The principal inference that the government will ask the jury to draw is that Mr. Soto was in the vicinity of the bank robbery when it occurred, was communicating with other alleged participants who were also in the vicinity of the bank, and that Mr. Soto therefore committed the bank robbery." *Id.* at 2.

This is not the first time that the government has proposed to use historical cell site location information as evidence in a criminal prosecution. In a case in the Eastern District of Pennsylvania, the government presented the expert testimony of a FBI agent who used cell site location information to attempt to map the movement of the defendant and to show that she was at a private residence. Testimony of FBI agent William B. Shute at 17-25 (*United States v. Sims*, No. 06-674 (E.D. Pa. Nov. 13, 2007)).<sup>10</sup> The agent testified that analysis of cell site information

---

<sup>8</sup> *Id.* at 616 (citing *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005)).

<sup>9</sup> *In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008).

<sup>10</sup> Available at <http://www.eff.org/files/filenode/celltracking/shutetestimony.pdf>. See also *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 Harv. J. L. & Tech. 307, 311 (2004) (describing how state used cell site location information in the Scott Peterson murder as evidence of the defendant's movements, including his presence at home).

over time can narrow the geographical area in which the phone is likely located, and that he has used the information close to 150 times to locate people such as fugitives. *See id.* at 16-18. He testified, for example, that the fact that the phone registered in alteration with two adjacent cell towers is “extremely consistent with the phone being somewhere in the middle of the two cell site sectors,” *id.* at 24. Conversely, according to the agent, the fact that the phone was consistently registering with the same cell site over a period of time “usually means that the phone is very close to the tower.” *Id.* at 23. In addition, he stated that where the phone registered with a series of different towers, it is likely that the person carrying the phone was on the move in a certain trajectory. *See id.* at 19-20, 21.

The government has thus previously taken the position, and will presumably take the position in this case, that cell site location information is sufficiently accurate as evidence of an individual’s whereabouts.

## **ARGUMENT**

The Fourth Amendment requires the government obtain a warrant based on probable cause and particular description to access cell site location information. This is because location tracking using cell site location information is a “search” under the Fourth Amendment that infringes on the reasonable expectation of privacy that Americans have traditionally enjoyed in their whereabouts. The fact that 90% of Americans now have cell phones which track this information does not sanction warrantless government access to this private information, but rather highlights the massive threat to Americans’ privacy if such information is not protected against government invasion.<sup>11</sup>

---

<sup>11</sup> *See* CTIA The Wireless Association, Wireless Quick Facts, <http://www.ctia.org/advocacy/research/index.cfm/AID/10323>.

**I. INDIVIDUALS HAVE A REASONABLE EXPECTATION OF PRIVACY IN THEIR LOCATION AND MOVEMENT INFORMATION.**

Cell site location information is protected by the Fourth Amendment because individuals have a reasonable expectation of privacy in their location and movement information, which can reveal intimate details of their lives—not only their presence in protected locations like their home, but their doctors’ visits, shopping habits, attendance at church, or association with others.

Over a quarter of a century years ago, the Supreme Court in *United States v. Karo*, 468 U.S. 705 (1984), held that location tracking implicates Fourth Amendment privacy interests because it may reveal information about individuals in areas where they have reasonable expectations of privacy. In *Karo*, the police placed a primitive tracking device known as a beeper inside a can of ether and used it to infer that the ether remained inside a private residence. In considering the Fourth Amendment challenge to the use of the beeper, the Court held that using an electronic device to infer facts about “location[s] not open to visual surveillance,” like whether “a particular article is actually located at a particular time in the private residence,” or to later confirm that the article remains on the premises, was just as unreasonable as searching the location without a warrant. *Id.* at 714-15.

*Karo* compels the conclusion that cell site location information implicates Fourth Amendment interests because, at minimum, just as the beepers of the *Karo* era, it reveals information about whether the cell phone is inside a protected location and whether it remains there. The cell phone travels through many such protected locations during the day where, under *Karo*, the government cannot warrantlessly intrude on individuals’ reasonable expectations of privacy. *See, e.g., Kyllo v. United States*, 533 U.S. 27, 31 (2001) (home); *See v. City of Seattle*, 387 U.S. 541, 543 (1967) (business premises); *Stoner v. California*, 376 U.S. 483, 486 (1964) (hotel room).

But the individual's privacy interest in his location information is not limited to the home or other protected locations: "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz v. United States*, 389 U.S. 347, 351 (1967). It is not only the cell phone's location in each constitutionally protected space, but the sum of the information gathered from the sweeping surveillance of a person's movement that reveals "precisely the kind of information that an individual wants and reasonably expects to be private." *W.D. Pa. 2008 (Lenihan)*, 534 F. Supp. 2d at 586 n.6. Indeed, the government in this case obtained cell site location information for 180 cell phones spanning over a period of time sufficient for it to attempt to retrace the defendant's historical movements and to attempt to show his association with other individuals. Mem. at 1-2.

Government access to this type of location and movement information implicates privacy concerns of a greater magnitude than the beepers of a quarter of a century ago. *Cf. United States v. Knotts*, 460 U.S. 276, 284-85 (1983) (permitting "limited" warrantless beeper use to aid the police in following a five-gallon container of chloroform during a single trip as it was moved in a car between two locations). First, as the Supreme Court has recognized, electronic surveillance that continuously and indiscriminately captures details of one's life "involves an intrusion on privacy that is broad in scope." *Berger v. New York*, 388 U.S. 41, 56-58 (1967). Individuals have the reasonable expectation of being free from such continuous and indiscriminate surveillance, even in areas potentially visible to the public. *See United States v. Cuevas-Sanchez*, 821 F.2d 248, 251 (5th Cir. 1987) (holding the indiscriminate video surveillance of an individual's backyard requires a warrant even if the police could have seen the backyard via a "one-time overhead flight or a glance over the fence by a passer-by"). As several state courts have acknowledged, location monitoring that is possible now, which by its nature is continuous

and indiscriminate, represents a far greater invasion of privacy than beepers which were monitored for as little as a day for the discreet purpose of ascertaining the destination of a particular object. *See, e.g., People v. Weaver*, 909 N.E. 2d 1195, 1198-99 (N.Y. 2009) (holding that the warrantless use of a GPS device, which, unlike the beepers of the past, “facilitates a new technological perception of the world in which the situation of any object may be followed and exhaustively recorded over . . . a practically unlimited period,” violated state constitution); *State v. Jackson*, 76 P.3d 217, 223 (Wash. 2003) (holding that the state constitution required a warrant for the two and one-half week, 24 hour surveillance of a GPS tracking device because “the intrusion into private affairs . . . is quite extensive”); *State v. Campbell*, 759 P.2d 1040, 1048 (Or. 1988) (holding that use of radio transmitter to locate defendant’s vehicle was a search under the state constitution, and stating that “[a]ny device that enables the police quickly to locate a person or object anywhere within a 40-mile radius, day or night, over a period of several days, is a significant limitation on freedom from scrutiny”).

Second, the technological progress heralded by cell site location information means that this form of tracking must be treated more restrictively than the beepers of the past because the technology is no longer tied to what can be ascertained through “naked-eye surveillance.” *Kyllo*, 533 U.S. at 33, 35 n.2 (holding that a warrant is required to use thermal imaging technology, which involves more than “naked-eye surveillance,” even if “equivalent information could be . . . obtained by other means,” for example by observing snowmelt on the roof); *cf. Knotts*, 460 U.S. at 285 (holding that the use of the beeper did not violate the Fourth Amendment where it did not reveal information that could not be obtained by visual surveillance); *Weaver*, 909 N.E. 2d at 1200 (“The science at issue in *Knotts* was . . . quite modest, amounting to no more than an incremental improvement over following a car by the unassisted eye.”); *Jackson*, 76 P.3d at 223



("[T]he GPS device does not merely augment the officers' senses, but rather provides a technological substitute for traditional visual tracking"). Accessibility of stored cell site location information at low cost permits the government to engage in surveillance of the magnitude that would not have been possible through visual surveillance. The facts here illustrate this point. Law enforcement would not have obtained the movement of 180 cell phones over a period of time through naked-eye surveillance, much less done so retrospectively.

The government may invoke cases in which courts have denied motions to suppress cell site and other cell phone location information.<sup>12</sup> These cases do not fully wrestle with individuals' reasonable expectations of privacy in location and movement information. These cases compare cell phone location information to beepers with little consideration of the greater Fourth Amendment interests at stake. The cases also rely on the third-party doctrine, which as explained below, is inapplicable here. *See infra* Part II.

The government may also attempt to argue that cell site location information is not sufficiently accurate to trigger Fourth Amendment scrutiny. Like beepers, however, cell site location information implicates Fourth Amendment concerns because, as explained above, it may reveal information that supports an inference of facts about a protected location, *see Karo*, 468 U.S. at 714-15; *Kyllo*, 533 U.S. at 36, and because it is no less sophisticated than beepers, *see, e.g., United States v. Berry*, 300 F. Supp. 2d 366, 368 (D.Md. 2004) ("[A] beeper is unsophisticated, and merely emits an electronic signal that the police can monitor with a receiver. The police can determine whether they are gaining on a suspect because the strength of

---

<sup>12</sup> *See, e.g., United States v. Forest*, 355 F.3d 942, 950-51 (6th Cir. 2004), *vacated on other grounds by, Garner v. United States*, 543 U.S. 1100 (2005); *United States v. Benford*, 2010 WL 1266507, \*2 (N.D. Ind. 2010); *United States v. Navas*, 640 F. Supp. 2d 256, 263 (S.D.N.Y. 2009), *rev'd in part on other grounds*, 597 F.3d 492 (2d Cir. 2010); *United States v. Suarez-Blanca*, 2008 WL 4200156, \*9 (N.D.Ga. 2008).

the signal increases as the distance between the beeper and the receiver closes”). Moreover, an argument from the government in this case that the information is too imprecise would be contradictory to the position it has taken in past cases, *see supra* Background III, and its intention to introduce this information as evidence. Given that it plans to argue that cell site location information is sufficiently accurate for supporting a finding of guilt beyond reasonable doubt, the government cannot argue for the purposes of the suppression motion that it is not precise enough to locate an individual or trace his movements.

In any event, the appropriate constitutional rule must be articulated with regard to “more sophisticated [technologies] that are already in use or in development.” *Kyllo*, 533 U.S. at 36. Future increases in the number of cell towers, as well as technology that is already available and used by the government like GPS and triangulation technology, will yield data that is more accurate than current cell site data.<sup>13</sup> It may be that the current cell site technology “is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations

---

<sup>13</sup> The number of active cellular towers is increasing by 11.5% each year, CTIA The Wireless Association, *CTIA’s Semi-Annual Wireless Industry Survey* at 9 (2009), available at [http://files.ctia.org/pdf/CTIA\\_Survey\\_Midyear\\_2009\\_Graphics.pdf](http://files.ctia.org/pdf/CTIA_Survey_Midyear_2009_Graphics.pdf), thus making cell site technology more accurate, *see Who Knows Where You’ve Been?*, *supra*, at 311 n.12 (“[T]he more cell towers available . . . the more precisely one’s movements can be tracked via cell towers”). Moreover, the government already requests more precise location information through existing technology like triangulation of information from multiple cellular towers and GPS technology. *See, e.g., In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 749 (S.D. Tex. 2005) (Smith) (triangulation); Letter from Executive Office for United States Attorneys to ACLU, December 31, 2008, available at [http://www.aclu.org/pdfs/freespeech/cellfoia\\_released\\_074135\\_12312008.pdf](http://www.aclu.org/pdfs/freespeech/cellfoia_released_074135_12312008.pdf) (stating, in a letter received as a result of a Freedom of Information Act lawsuit filed by *Amici* against the United States Attorneys Office for the Southern District of Florida, that six applications to “obtain GPS or similarly precise location data” were granted after November 16, 2007, without a judicial determination of probable cause).

from legal modes of procedure.” *Silverman v. United States*, 365 U.S. 505, 512 (1961) (internal quotation marks omitted).

The facts of this case demonstrate that the government is already using the available cell site technology not only to retrace the movements over time of those suspected of involvement in a crime, but to review the movement and associations of 180 individuals, some of whom could not have any possible connection to the investigation. These facts illustrate that “dragnet type law enforcement practices” that threaten to eviscerate privacy rights and chill associational and other expressive activities are now a reality. *Knotts*, 460 U.S. at 283-84 (reserving for another day the constitutionality of dragnet type law enforcement practices like twenty-four hour surveillance); *United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007) (permitting warrantless GPS tracking when the police have a suspect in their sights, but stating that “[t]echnological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive” and reserving decision on constitutionality of programs of mass surveillance), *cert. denied*, 552 U.S. 883 (2007); *W.D. Pa. 2008 (Lenihan)*, 534 F. Supp. 2d at 612 (“[N]ewly-emergent technologies create the potential to monitor associational activities in a manner that could have a chilling effect”).

The Fourth Amendment protects an individual’s reasonable expectations of privacy in information that he “seeks to preserve as private.” *Katz*, 389 U.S. at 351. It cannot be correct that that Amendment has nothing to say about whether government, enabled by technology, may subject Americans to round-the-clock surveillance of their movements for as long as it likes.

**II. THAT THE CELL PHONE PROVIDER, A THIRD-PARTY, HAS ACCESS TO CELL SITE LOCATION INFORMATION DOES NOT UNDERMINE THE CELL PHONE USERS' REASONABLE EXPECTATION OF PRIVACY IN THEIR LOCATION AND MOVEMENT INFORMATION.**

The 90% of the American public that uses a cell phone maintain their reasonable expectation of privacy in their location and movement information because the cell phone providers' collection of cell site location information has little to do with the so-called "third-party doctrine," which holds that a person loses her expectation of privacy in information when she voluntarily communicates it to a third-party. *See Smith v. Maryland*, 442 U.S. 735, 743-44 (1979); *United States v. Miller*, 425 U.S. 435 (1976). Those cases were decided on the notion, inapplicable here, that by knowingly and voluntarily disclosing this information, she assumes the risk that the third-party will reveal the information to others. *See Smith*, 442 U.S. at 743-44.

Unlike those third-party doctrine cases, cell phone users do not knowingly and voluntarily take the risk of having their location information revealed to the public. For example, unlike the phone numbers dialed by the telephone user in *Smith*, cell site location information is not information that the user directly conveys to an operator orally or dials on his phone in order to connect the call. That information is generated and recorded automatically by the interaction of cell phones and the cell towers, in response to initiation of calls and receipt of calls. It is also generated every seven seconds regardless of the individual's use of the phone. *See W.D. Pa. 2008 (Lenihan)*, 534 F. Supp. 2d at 589-90. That cell site location information is generated without his knowledge means that he has not voluntarily and knowingly communicated this information to the public. *See id.* at 615 ("[Cell site data] is not 'voluntarily and knowingly' conveyed (certainly *not* in the way of transactional bank records or dialed numbers); rather, the information is automatically registered by the cell phone."); *S.D. Tex. 2005 (Smith)*, 396 F. Supp. 2d at 756-57 ("[Unlike dialed numbers, cell site data] is transmitted

automatically during the registration process, entirely independent of the user's input, control, or knowledge.”).

In addition, unlike the phone numbers in *Smith*, this information typically does not appear in a cell phone user's bill, thus providing users with no subjective awareness that the information is being generated and recorded. *Cf. Smith*, 442 U.S. at 742 (“All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.”).

Finally, in the world where massive quantity of personal information is stored or processed by businesses, the third-party doctrine must have its limits. The Supreme Court has recognized as much. The Court has concluded, for example, that individuals have a reasonable expectation of privacy in the content of their telephone calls, *see Katz*, 389 U.S. at 352-53, even though “[t]he telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment.” *Smith*, 442 U.S. at 746 (Stewart, J., dissenting).

Like the contents of a communication, cell site location information is personally revealing and people reasonably expect privacy in their movements. *See supra* Part I. In its continuous and indiscriminate nature, cell phone tracking raises Fourth Amendment concerns similar to the surveillance of the content of conversations. *Cf. Berger*, 388 U.S. at 56-58. The third-party doctrine does not extend to such intimate information, particularly when an individual has done little to voluntarily convey the information to a third party.

**III. BECAUSE CELL PHONE TRACKING IS A SEARCH, LAW ENFORCEMENT MUST OBTAIN A WARRANT BASED ON PROBABLE CAUSE AND PARTICULAR DESCRIPTION TO ACCESS CELL SITE LOCATION INFORMATION.**

Because cell site location information implicates an expectation of privacy that society is prepared to recognize as reasonable, the Fourth Amendment requires that the government obtain a warrant based on probable cause prior to collecting this information. Furthermore, the constitutional requirement of particularity mandates that, because cell site location information implicates surveillance that is continuous and indiscriminate, the government: (1) obtain certification by a judge that “normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous,” (2) provide “a particular description of the type of [information] sought . . . and a statement of the particular offense to which it relates,” (3) state a period of surveillance that is no “longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days (though renewals are possible),” and (4) conduct the surveillance “in such a way as to minimize the [collection of information] not otherwise subject to surveillance.” *United States v. Torres*, 751 F.2d 875, 883-84 (7th Cir. 1984) (internal citations omitted) (adopting the four requirements for video surveillance) (Posner, J.), *cert. denied*, 470 U.S. 1087 (1985). “Each of these four requirements is a safeguard against electronic surveillance that picks up more information than is strictly necessary.” *Id.* at 884. These requirements were first articulated by the Court in *Berger* in the context of eavesdropping, *Berger*, 388 U.S. at 55-60, have since been codified in Title I of the ECPA governing wiretapping, *see* § 2518, and have been uniformly adopted by courts, including the Second Circuit, in evaluating the constitutionality of video surveillance, *see, e.g., Torres*, 751 F.2d at 885; *United States v. Biasucci*, 786 F.2d 504, 510 (2d Cir. 1986), *cert.*

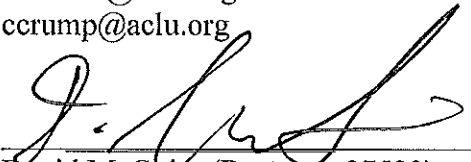
*denied*, 479 U.S. 827 (1986).<sup>14</sup> Because cell site location monitoring is just as continuous and indiscriminate as eavesdropping, wiretapping, and video surveillance, a warrant for this type of surveillance must also meet the four particularization requirements in Title I, *see* § 2518(3)(c), § 2518(4)(c), § 2518(5).

Because the government failed to comply with Fourth Amendment requirements by obtaining a warrant, the cell site location information in this case should be suppressed.<sup>15</sup>

Respectfully submitted,

/s/ Mariko Hirose

Mariko Hirose, *pro hac vice pending*  
Catherine Crump, *pro hac vice pending*  
American Civil Liberties Union  
125 Broad Street, 17th floor  
New York City, NY 10004  
(212) 549-2604  
FAX: (212) 549-2651  
mhirose@aclu.org  
ccrump@aclu.org



David McGuire (Bar no. ct27523)  
ACLU of Connecticut  
2074 Park St., Suite L  
Hartford, CT 06106  
(860) 523-9146 Ext. 212  
FAX: (860) 586-8900  
dmcguire@acluct.org

---

<sup>14</sup> *See also, e.g., United States v. Falls*, 34 F.3d 674, 680 (8th Cir. 1994), *cert. denied*, 534 U.S. 879 (2001); *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992) (en banc), *cert. denied*, 506 U.S. 1005 (1992); *United States v. Mesa-Rincon*, 911 F.2d 1433, 1437-38 (10th Cir. 1990); *Cuevas-Sanchez*, 821 F.2d at 252.

<sup>15</sup> In order to comply with its constitutional obligations, the government could have and should have applied for a warrant under the SCA to obtain historical cell site location information. The SCA, by its plain language, permits the government to access “a record or other information pertaining to a subscriber to or customer of [an electronic communication] service”—which includes a stored record like cell site location information—upon obtaining a Rule 41 warrant. 18 U.S.C. § 2703(c)(1).

Kevin S. Bankston, *pro hac vice pending*  
Jennifer Granick, *pro hac vice pending*  
Electronic Frontier Foundation  
454 Shotwell Street  
San Francisco, CA 94110  
(415) 436-9333 x126  
bankston@eff.org  
jennifer@eff.org

Scott Michelman, *pro hac vice pending*  
American Civil Liberties Union  
1101 Pacific Avenue, Suite 333  
Santa Cruz, CA 95060  
(831) 471-9000 ext. 31  
FAX: (831) 471-9676  
smichelman@aclu.org



## CERTIFICATE OF SERVICE

This is to certify that on this 18th day of June, 2010, a copy of the foregoing Unopposed Motion of the American Civil Liberties Union (ACLU), ACLU of Connecticut, and Electronic Frontier Foundation for Leave to Submit *Amici Curiae* Brief was filed and served by email to all parties. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system or by mail to anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing. Parties may access this filing through the Court's CM/ECF System.

A handwritten signature in black ink, appearing to read 'D. McGuire', written over a horizontal line.

David McGuire