September 23, 2005

Via Electronic Filing

The Honorable James Orenstein
United States Magistrate Judge
Eastern District of New York
Long Island Federal Courthouse
924 Federal Plaza
Central Islip, New York 11722-4454

RE: Letter Brief of *Amicus Curiae* The Electronic Frontier Foundation Opposing the Government *In re Application for Pen Register and Trap and Trace Device With Cell Site Location Authority*, Magistrate's Docket No. 05-1093 (JO)

Dear Magistrate Judge James Orenstein:

The Electronic Frontier Foundation ("EFF") respectfully submits this *amicus curiae* brief in opposition to the Government's pending motion to reconsider the Memorandum and Order entered August 25, 2005 (the "August 25 Order"), __ F.Supp.2d __, 2005 WL 2043534 (E.D.N.Y. 2005). EFF supports the issuance of an amended order rejecting the new argument raised in the Government's motion: that this Court may combine an order under 18 U.S.C. § 3123 to an order under 18 U.S.C. § 2703(d), and issue a hybrid order authorizing surveillance that neither statute allows. There is no support for this statutory chimera in the statutes' text or legislative history, nor in any published case or legal commentary. Additionally, such an order would fail to satisfy the Fourth Amendment's restrictions on such surveillance. Therefore, the August 25 Order properly denied the Government's application, and the Government's motion for reconsideration should also be denied.

I. Statement of Interest

EFF is a member-supported, non-profit legal foundation that litigates to protect free speech and privacy rights in the digital age. As part of that mission, EFF has served as counsel or amicus in key cases addressing the Electronic Communications Privacy Act ("ECPA") and its component the Stored Communications Act ("SCA"), as well as the Communications Assistance for Law Enforcement Act ("CALEA") and related electronic privacy statutes. *See, e.g., Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994); *U.S. Telecom Ass'n v. F.C.C.*, 227 F.3d 450 (D.C. Cir. 2000); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002), *cert. denied*, 537 U.S. 1193 (2003); and *U.S. v. Councilman*, 418 F.3d 67 (1st Cir. 2005).

II. Introduction

This matter involves two applications made by the Government: first, an application made under 18 U.S.C. § 3122 for an order under 18 U.S.C. § 3123 authorizing installation of a pen register or

trap and trace device (an application for a "Pen-Trap Order" under the "Pen-Trap Statute" to install a "Pen-Trap Device"); second, an application for an order issued under 18 U.S.C. § 2703(d) of the Stored Communications Act (a "D Order" under the "SCA"), requiring an electronic communications service provider to disclose "records or other information pertaining to a subscriber or customer." 18 U.S.C. § 2703(c)(1). Pen-Trap Orders are issued based only on the Government's certification of relevance to an ongoing criminal investigation, *see* 18 U.S.C. § 3123(a), while a D Order requires a showing of specific and articulable facts giving reasonable grounds to believe the records sought are relevant and material to the investigation. *See* 18 U.S.C. § 2703(d).

Based on this joint application, the Government seeks an order authorizing installation of a Pen-Trap Device to prospectively collect cell site information and thereby monitor the location of a particular cell phone when it is in use. August 25 Order at *2, Gov't Motion at 2-3. Apparently, the Government originally attempted to obtain such an order without explicit reliance on the Pen-Trap Statute, instead seeking to accomplish its goals via a D Order alone. *See* August 25 Order at *1-2. Faced with unexpected resistance, the Government belatedly concedes that neither a Pen-Trap nor D Order alone could authorize it to track a cell phone's location. *See* Gov't Motion at 2-3, 6-7. Instead, the Government now argues the equally unsupported proposition that it seeks an order based on the combined authority of the Pen-Trap Statute and the SCA. *See id.* at 5-6.

III. Argument

A. Court Order Issued Under 18 U.S.C. § 2703(d) Cannot Authorize or Compel the Prospective Collection of Information.

Section 2703 of the SCA applies only to the disclosure of existing information and not to prospective surveillance. The Government explicitly concedes that a D Order would not suffice in this case: "That is not to say that the order we propose could or should issue based solely on the SCA." Gov't Motion at 7. The SCA provides in relevant part:

> A governmental entity may require a provider of electronic communication service… to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity… obtains a court order for such disclosure under subsection (d) of this section.

18 U.S.C. § 2703(c).[1] The Government argues and we will assume *arguendo* that cell site information constitutes such a "record or other information," *see* Gov't Motion at 6, and there is

[1] The Government has apparently abandoned its argument that cell location data would be included in the narrower, less-protected class of specified non-content records and information obtainable via subpoena under 18 U.S.C. § 2703(c)(2). *See* August 25 Order at *1 (noting

no dispute that a cell phone provider is a provider of electronic communication service and the Government is a governmental entity. Accepting these premises, then, why does the Government not argue that the plain language of Section 2703 already authorizes a D Order for prospective cell site information even absent an accompanying Pen-Trap Order?

The Government does not make such an argument because it recognizes, as it must, that the "records or other information" governed by the SCA are *retrospective*, and that Section 2703 does not apply to the *prospective* collection of any information, but only to the disclosure of existing records. Indeed, the Government concedes that point when arguing for its hybrid:

> 18 U.S.C. § 2703 authorizes the Court to order cellular telephone providers to disclose *existing* cell-site usage records. In addition, the Court is authorized to order disclosure of cell-site information on a *prospective* basis where, as here, the government's application is made *not only* under authority of SCA, but also under the Pen/Trap statute….

Gov't Motion at 2 (emphasis added).

As the Government has further explained in its own electronic evidence manual: "Any *real-time* interception of electronically transmitted data in the United States must comply strictly with the requirements of Title III, 18 U.S.C. §§ 2510-2522 [The Wiretap Act], or the Pen/Trap statute, 18 U.S.C. §§ 3121-3127," while "18 U.S.C. §§ 2701-12 [the SCA]… governs how investigators can obtain *stored* account records and contents …." U.S. Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* at ix, 24 (July 2002), *available at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf (emphasis added). Academic and industry commentators have uniformly recognized the same statutory distinction between retrospective and prospective surveillance.[2] This consensus is unsurprising considering that the SCA's applicability to stored information rather than prospectively collected

---

Government's reliance on Section 2703(c)(2)), and Gov't Motion at 3 ("the controlling authority" is Section 2703(c)(1)(B).) That argument contradicts the Government's current position that CALEA specifically allows Pen-Trap Orders for location tracking only if they are issued under the "intermediate standard" of a D Order. *See* Gov't Motion at 5.

[2] *See, e.g.*, U.S. Internet Service Provider Association, *Electronic Evidence Compliance—A Guide for Internet Service Provider*s, 18 BERKELEY TECH. L.J. 945, 951, 957 (2003) (D Orders are for "historical" non-content records, while Pen-Trap Orders are for "any prospective non-content information….") and Deirdre Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1565 (2004) ("The Wiretap Act and Pen Register statute regulate prospective surveillance… and the SCA governs retrospective surveillance…."); *see generally* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 46-52 (2004) (providing overview of different categories of surveillance).

information is clearly reflected in its title and in the title of the code chapter that contains it, i.e., "Chapter 121—Stored Wire and Electronic Communications and Transactional Records Access." *See* Pub.L. 99-508, Title II, § 201, Oct. 21, 1986, 100 Stat. 1860.

By definition, "records" are historical,[3] so the Government relies instead on the word "information" in the phrase "record or other information." *See* Gov't Motion at 2. Read in context, however, the "other information" in addition to "records" is also limited to already-existing information, and clarifies that the SCA protects all stored information pertaining to a subscriber regardless of any quibbling over what constitutes a "record." It is also clear from the types of records and information specified in Section 2703(c)(2) that Congress on occasion uses "record" and "information" to refer to slightly different classes of *historical* data,[4] when it is not using the terms interchangeably.[5]

The legislative history's repeated reference to "records" being "maintained," "kept," or "stored" further demonstrate that the SCA was only intended to govern existing records and information, not to authorize prospective information-gathering. *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); and 132 Cong. Rec. H4039-01 at __ , 1986 WL 776505 (1986) (Statement of bill sponsor, Rep. Robert W. Kastenmeier, emphasizing 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.").

The absence of any provision requiring the technical assistance necessary for prospective collection reinforces the fact that the SCA applies only to stored information. Both the Wiretap Act and the Pen-Trap Statute, which authorize the prospective collection of communications content and non-content information, respectively, specifically provide for orders compelling

---

[3] A "record" is "an account, as of information or facts, set down especially in writing as a means of preserving knowledge," "information or data on a particular subject collected and preserved," or "the known history of performance, activities, or achievement." *American Heritage Dictionary of the English Language*, 4th Ed. (2000), *available at* http://www.dictionary.com.

[4] "Records[s] or other information" obtainable via subpoena under 18 U.S.C. § 2703(c)(2) include two classes: discrete pieces of "information" such as subscriber name, address, and credit card number, as well as "records" that constitute a historical log of repeated or continued activity, e.g., "local and long distance telephone connection records, or records of session times or durations." *Id.*

[5] E.g., 18 U.S.C. § 2703(c)(1)(E) refers to the records and information available under 18 U.S.C. § 2703(2) as "information" only, even though it explicitly provides access to particular "records," and the title of 18 U.S.C.§ 2703 refers only to "records concerning electronic communication service," even though the section applies to "records and other information." *Id.*

communications service providers to give the Government whatever "information, facilities or technical assistance" necessary to implement the authorized surveillance. *See, e.g.*, 18 U.S.C. § 2511(2)(a)(ii). Under the Wiretap Act, "a court order directing such assistance [must be] signed by the authorizing judge," "set[] forth the period of time during which the provision of the information, facilities, or technical assistance is authorized," and "specify[] the information, facilities, or technical assistance required." *Id*. A Pen-Trap Order, meanwhile, "shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device…." 18 U.S.C. § 3123(b)(2); *see also* 18 U.S.C. § 3124 (the required assistance "include[es] installation and operation of the device….").

In contrast, the SCA does not provide for any order compelling such assistance, and a D Order can only command "disclosure" of the materials sought. 18 U.S.C. § 2703(d). Indeed, the lack of this authority under the SCA, and its presence in the Pen-Trap Statute, is likely one of the Government's main reasons for seeking to wed a D Order with a Pen-Trap Order. Congress, however, never blessed such a union.

B. There is No Authority Allowing an Order under 18 U.S.C. § 2703(d) to Be Combined With a Pen-Trap Order for the Purpose of Prospectively Collecting Location Information.

A D Order cannot order the disclosure of location information on a prospective basis or require the installation of a device, as demonstrated above. Furthermore, as this Court properly held, *see* August 25 Order at *3, and the Government has since conceded, *see* Gov't Motion at 2-3, Congress has forbidden the prospective disclosure of location information based on a Pen-Trap Order. *See* 47 U.S.C. § 1002(a)(2)(B) ("[I]nformation 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."). Yet the Government persists, attempting to convince the Court that one insufficient order in combination with another insufficient order is somehow sufficient.

As an initial matter, neither the text of the Pen-Trap Statute nor the SCA acknowledges the existence of such a hybrid order, whether implicitly or explicitly. There is simply no evidence of Congressional intent that the two statutes could, in combination, authorize a location-tracking order. In fact, the legislative history of CALEA suggests that the Government cannot use a Pen-Trap Device to obtain location data *at all*, regardless of what type of order is used: "The bill," Congress explained, "protects privacy…by restricting the ability of law enforcement to use pen register *devices* for tracking purposes…." H.R. Rep. No. 103-827, 103d Cong., 2d Sess., pt. 1, at 12 (1994), reprinted in 1994 U.S.C.C.A.N. 3489 (emphasis added). Yet, as the Government concedes, the location information sought "requires installation of a pen register." Gov't Motion at 6. The Government's interpretation of the statutory scheme therefore ignores Congress' clear intent to prohibit the collection of location information using Pen-Trap Devices, instead

contending that Congress' use of the word "solely" in Section 1002 of CALEA contains a hidden exception to this rule.

The Government appears to subscribe to a "clown car" theory of statutory interpretation: from one tiny word, meanings spill out in multitudes. It argues that the prohibition against the collection of location data "solely" pursuant to the Pen-Trap Statute's authority is actually an implicit authorization for the use of Pen-Trap Devices to prospectively collect location data, where a Pen-Trap Order is combined with a D Order. Gov't Motion at 6-7. The Government offers only one justification for this interpretive leap, arguing that Congress somehow had a Pen Trap plus D Order in mind when it wrote "solely" into CALEA because D Orders were also created by CALEA. Gov't Motion at 4-5.

The fact that Congress wrote these provisions at the same time cuts against the Government's argument: if two provisions of the same Act were as intimately intertwined as the Government suggests, Congress would have made the connection explicit. Congress' stated purpose in creating D Orders was not to provide complementary authority to the Pen-Trap Statute for purposes of location tracking in contradiction to CALEA's clear prohibition on the use of Pen-Trap Devices for that purpose. Rather, its stated purpose was to protect privacy by preventing the Government from being able to obtain a "person's entire on-line profile" with only a subpoena. H.R. Rep. 103-827 at 19.

The Government, however, has maintained in proceedings before the FCC that CALEA "embodies a compromise regarding location information" where law enforcement can "acquire location information under other electronic surveillance statutes." *In the Matter of Communications Assistance for Law Enforcement Act*, 14 F.C.C.R. 16794 at ¶ 42 (1999). Neither the statute's plain language nor the legislative history refer to such a compromise, and the Government's oblique references to back-room deals cannot form the basis of statutory interpretation. But even if we assume *arguendo* that such a deal took place, CALEA forbids the use of the Pen-Trap Statute and the only other authorized electronic surveillance available is under the Wiretap Act. *See U.S. Telecom Ass'n v. F.C.C.*, 227 F.3d 450 at 454 (D.C. Cir. 2000) (quoting H.R. Rep. 103-827 at 14-15 ("authorized electronic surveillance" refers to "wiretaps, pen registers and trap and traces.")). Therefore, even assuming *arguendo* that Congress did intend some type of hybrid order based on multiple electronic surveillance statutes, the only remaining statutory authority available to law enforcement is the Wiretap Act, which is also the only statutory authority that would satisfy the Fourth Amendment's requirements.

C. Only a Warrant Satisfying the Wiretap Act's Core Requirements Can Authorize the Proposed Surveillance.

The Supreme Court has only permitted warrantless location tracking where the information revealed could have been obtained by visual surveillance from public places. *See United States v. Knotts*, 460 U.S. 276 (1983) (evaluating whether monitoring of "beeper" attached to large drum of chemicals in suspect's possession violated Fourth Amendment) and *United States v.*

Karo, 468 U.S. 705 (1984) (same). In *Knotts*, there was no evidence that the beeper was monitored while it was inside the suspect's home. The Court thus concluded that the beeper yielded only information about the drum's movements in public, information that could have been obtained visually without implicating any privacy interest. *See* 460 U.S. at 277, 282, 285 ("Visual surveillance from public places along the [suspect's] route" on public roads would have revealed the drum's movements; Fourth Amendment was not implicated "because a police car following [the suspect's car] at a distance could have observed…the [five-gallon] drum of chloroform still in the car.").

In contrast, where the beeper was monitored while inside the suspect's home and revealed the drum's location even when not exposed to the public, the Court found that the warrantless surveillance violated the Fourth Amendment. *See Karo*, 468 U.S. at 714. The court further found that the Government must "obtain warrants prior to monitoring a beeper when it has been withdrawn from public view." *Id.* at 718. Given that law enforcement cannot know when that will occur, "warrants for the installation and monitoring of a beeper will obviously be desirable since it may be useful, even critical, to monitor the beeper to determine that it is actually located in a place not open to visual surveillance." *Id.* at 713 n.3.

The cell phone at issue in the present case is not at all like a five gallon drum. A cell phone is a pocket-sized device that is routinely carried within the home, and often carried on one's person in public such that it is not in public view. The prospective collection of cell site data will therefore reveal the cell phone's location even when that information could not have been derived from visual surveillance, but only from a physical search.[6] Under *Karo*, the Fourth Amendment requires a warrant for such invasive surveillance.

Cell phone tracking additionally endangers individuals' Fourth Amendment privacy interests in ways that echo the Supreme Court's concerns about eavesdropping: the surveillance is ongoing,

---

[6] A simple hypothetical makes the point: the suspect, under visual surveillance, is seen holding the target phone as he enters his home. Inside the house, he gives the phone to his teenage daughter who is going to a sleepover, and she puts it in her backpack. She then drives to her friend's house across town. Once inside, she takes the phone out of her bag and calls her father to say she arrived safely.

Even assuming *arguendo* the wholly unsupported proposition that cell tracking could only reveal the phone's "general vicinity," Gov't Motion at 8, the Government has still learned that the phone was removed from the home based on the daughter's call. That information was never revealed in public view and could only have been obtained by a physical search of the home (or the friend's home, or the daughter's backpack), subject to the Fourth Amendment. One "may not find that information particularly private or important"—certainly, the Government is most interested in the suspect's movements, not the phone's—"but there is no basis for saying it is not information regarding the interior of the home." *Kyllo v. United States*, 533 U.S. 27, 35 n.2 (2001).

surreptitious, and lacks particularity. *Berger v. New York*, 388 U.S. 41, 59 (1967) (equating two-month eavesdropping order to "a series of intrusions, searches, and seizures"); *id*. at 60 (insisting on "some showing of special facts" to cure "defect" of not requiring notice); *id*. at 62 ("indiscriminate use of [electronic monitoring] devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments") (citation and internal quotation marks omitted). Congress designed the Wiretap Act to cure the constitutional defects identified in *Berger*: Not only must Wiretap Orders be based on a judicial finding of probable cause and describe the surveillance with particularity, the particular crime must be specified, there must be clear time limits, less intrusive means must be unavailable, and the collection of irrelevant information must be minimized. *See* 18 U.S.C. § 2518. Accordingly, "[The Wiretap Act] does not suffer from the infirmities that the Court found fatal to the statute in *Berger*." *United States v. Tortorello*, 480 F.2d 764, 775 (2d Cir. 1973), *cert. denied*, 414 U.S. 866 (1973), and therefore provides an appropriate model for evaluating the surveillance at issue here.

The Government's argument that the privacy interest here is most analogous to that in *Smith v. Maryland*, 442 U.S. 735 (1979), is unpersuasive. First, the Government mischaracterizes as minimal the privacy invasion posed by cell phone tracking, arguing that it can only reveal one's "general vicinity." Gov't Motion at 8. This assertion is unsupported, and contradicts the Government's own concession that CALEA's provision regarding "information that may disclose the physical location of the subscriber" applies to the information it seeks. *Id.* at 7. The Government also omits to mention that information from multiple cell towers can be used to triangulate a phone's specific location. See 14 F.C.C.R. 16794 at ¶ 46 (1999) (rejecting due to privacy concerns an NYPD proposal that the FCC require telecommunications providers under CALEA to provide Government with capability to triangulate signals from multiple cell towers and thereby pinpoint a phone's precise location throughout a call's duration). Indeed, federal law *requires* that cell phone providers whose phones do not contain GPS chips or similar "handset-based" tracking technologies be able to use "network-based" methods such as cell triangulation to locate a cell phone to within at least 100 meters for most calls, so that emergency services can locate 911 callers. *See* 47 C.F.R. 18(h).

Smith v. Maryland's finding of no Fourth Amendment privacy interest in dialed phone numbers was premised on the holding that "all telephone users realize that they must convey phone numbers to the telephone company." 442 U.S. at 742; *see also id.* at 742-43 (reciting the facts supporting that holding) (internal quotation marks omitted). In contrast, the Government in this case can offer no evidence that all or even most cell phone users realize that they are conveying their locations to the telephone company. Absent such evidence, and in order to ensure individual privacy against unreasonable invasion, this Court must assume based on *Karo* and *Berger* that the Fourth Amendment protects this information and require that the Government satisfy the *Berger*-derived requirements of the Wiretap Act.

Adherence to these core requirements of the Wiretap Act in the present case is consistent with the circuit courts' approach when considering novel issues of electronic surveillance that implicate the Fourth Amendment. Amicus respectfully urges the Court to follow the lead of

those courts, which have uniformly applied the core requirements of the Wiretap Act to video surveillance even though the Wiretap Act does not by its terms address the practice. *See United States v. Biasucci*, 786 F.2d 504 (2d. Cir. 1986), *cert. denied*, 479 U.S. 827 (1986); *United States v. Torres*, 751 F.2d 875 (7th Cir. 1984), *cert. denied*, 470 U.S. 1087 (1985); *United States v. Cuevas-Sanchez*, 821 F.2d 248 (5th Cir. 1987); *United States v. Mesa-Rincon*, 911 F.2d 1433 (10th Cir. 1990); and *United States v. Koyomejian*, 970 F. 2d 536, *cert. denied*, 506 U.S. 1005 (1992); *see generally* Freiwald, 56 ALA. L. REV. at 72. In ECPA's legislative history, Congress approved of this approach as providing "legal protection against the unreasonable use of newer surveillance techniques." H.R. Rep. No. 99-647 at 18, 18 n.11. Such protection is plainly needed here, and neither a Pen-Trap Order, a D Order, nor some ill-conceived combination of the two will suffice.

For the above reasons, EFF respectfully requests that this Court deny the Government's motion for reconsideration.

Respectfully submitted,

By: _____

Wendy Seltzer (WS-4188)
250 Joralemon Street
Brooklyn, NY 11201
Telephone: (917) 780-7961
Facsimile: (917) 780-0934
wendy@seltzer.org

Kevin Bankston, EFF Staff Attorney
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x 126
Facsimile: (415) 436-9993
bankston@eff.org

ATTORNEYS FOR AMICUS CURIAE
ELECTRONIC FRONTIER FOUNDATION

cc: Burton T. Ryan, Jr.
Assistant U.S. Attorney
United States Attorney's Office
610 Federal Plaza
Central Islip, NY 11722-4454