December 6, 2005

Via Hand Delivery

Honorable Andrew J. Peck
Chief United States Magistrate Judge
Southern District of New York
United States Courthouse
500 Pearl Street, Room 750
New York, New York 10007

RE: In re Government Application for Pen Register and Trap and Trace Device with Cell-Site Location Authority

Dear Chief Magistrate Judge Peck:

Amicus the Federal Defenders of New York ("FDNY"), joined by the Electronic Frontier Foundation ("EFF"),[1] writes to reply briefly to the government's letter of Nov. 22, 2005 ("Gov. Br. II") and to advise the Court of a timely decision that can inform the present controversy: In re Application of United States for an Order Authorizing Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers [Sealed] and [Sealed] and the Production of Real Time Cell Site Information, ___ F. Supp. 2d ___, 2005 WL 3160860 (D.Md. Nov. 29, 2005) ("Bredar Op."). The basic holding of that decision, as of the previous decisions on point, can be summed up in one sentence: No existing statutes authorize real-time collection of cell-site data.

I. No existing statutes authorize real-time collection of cell-site data.

The latest decision to address real-time cell-site tracking cuts through the oft-cited complexity of the federal surveillance statutes and the seeming novelty of the issues presented, and quickly reaches the simple heart of the matter: "[t]he issue presented by this application is whether *existing statutes* allow the government to obtain real time cell site information upon a showing of less than probable cause." Bredar Op. at *1 (emphasis added).

Magistrate Judge Bredar, like Magistrate Judges Orenstein and Smith before him, determined that existing statutes do *not* authorize such surveillance, leaving the court with "only its

[1] Statement of Interest of *Amicus* EFF: 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 surveillance statutes at issue here. 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). EFF also served as *amicus* to Judge Orenstein when he recently considered a cell-site application in the Eastern District of New York.

general authority to issue a Rule 41 warrant upon a showing of probable cause." Id.; see also In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, ___ F. Supp. 2d ___, 2005 WL 2656621 (S.D.Tx. Oct. 14, 2005) ("Smith Op."); and In re Application of the United States for an Order (1) Authorizing Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 384 F. Supp. 2d 562 (E.D.N.Y. Aug. 25, 2005) ("Orenstein Op. I"), on reconsideration, ___ F. Supp. 2d. ___, 2005 WL 2739208 (E.D.N.Y. Oct. 24, 2005) ("Orenstein Op. II"). The government has not appealed these decisions despite the courts' strongest encouragement. See, e.g., Smith Op. at *16 (Court's opinion "was written in the full expectation and hope that the government will seek appropriate review by higher courts…."). Yet the government here, and presumably before other courts, continues to press the same arguments that have been definitively rejected in every published decision to address them.

As three courts have now explained the insufficiency of the existing statutes at length, *Amici* will here only briefly summarize the essence of those decisions. However, *Amici* will gladly provide further briefing if the Court requests it.

A. The Pen-Trap Statute does not authorize real-time cell-site tracking.

The government concedes and the three courts have agreed that Congress has forbidden the real-time collection of cell-site information pursuant solely to the "Pen-Trap Statute," see 18 U.S.C. §§ 3121 et seq., regardless of whether cell-site data constitutes "dialing, routing, addressing or signaling information" as the government argues. See Orenstein Op. II at *11-12; Smith Op. at *9; Bredar Op. at *5; Gov. Br. II at 2, 7-11; and government's letter of October 5, 2005 ("Gov. Br. I") at 7-9.

B. Section 2703 of the Stored Communications Act does not authorize real-time cell-site tracking.

The three courts have also agreed that orders issued under 18 U.S.C. § 2703(d) of the Stored Communications Act (the "SCA") cannot authorize *real-time*[2] acquisition of any information, based on the statute's plain language, structure, and legislative history. See Smith Op. at *11-12; Orenstein Op. II at *13-14, *17-18; and Bredar Op. at *4. This reading holds regardless of whether an order under Section 2703(d) can demand *historic* cell-site information. See Smith Op. at *11 n.16 (noting that Section 2703(d) may reach historic cell-site information); Orenstein Op. II at *16-17 (finding that a Section 2703(d) order can demand existing cell-site

[2] Judge Bredar limited his holding to "real time" acquisitions, which he considered to be a subset of "prospective" acquisitions, though noting that the same logic likely applied to all prospective surveillance. See Bredar Op. at *2, 7 n.11. By Judge Bredar's terms, Judges Orenstein and Smith both held that Section 2703(d) cannot authorize any form of prospective surveillance, because such orders can only demand *existing* records. See Orenstein Op. II at *17 and Smith Op. at *11-12. *Amici* agree with Judges Orenstein and Smith on this point.

information); Bredar Op. at *4 (reserving question of Section 2703's applicability to historic cell-site information).

The courts' consensus is consistent with the understanding of industry and academic commentators,[3] as well as the government's own last publicly available surveillance manual.[4] Indeed, as far as *Amici* can determine, the government's briefing in the recent spate of cell-site cases is the first and only time anyone has publicly argued that possibility that an order issued under Section 2703(d) could authorize real-time surveillance.

Although the courts' consensus and the complete lack of contrary authority is more than persuasive, the government refuses to concede that orders under Section 2703(d) may demand records only retrospectively. See Gov. Br. II at 12-13, 15-16. The government's persistence here is probably due to its apparent previous practice of seeking cell-site orders for real-time surveillance under Section 2703 alone. See Smith Op. at *12 (original application did not cite Pen-Trap Statute as authority for cell-site order); Orenstein Op. II at *4 (same); Bredar Op. at *1 (failing to specify the statutes referenced in the application but citing Section 2703(d)).

C. The Pen-Trap Statute and Stored Communications Act do not in combination authorize real-time cell-site tracking.

Neither the relevant statutes' plain language nor legislative history supports the government's proposal that this Court marry the Pen-Trap Statute to the SCA in order to issue a cell-site order. The previous decisions have exhaustively catalogued the arguments against this "undeniably creative" but absolutely "perverse" theory. See Smith Op. at *12-16, Orenstein Op. II at *20-26, and Bredar Op. at *5. As Judge Orenstein observed, the theory is likely a

---

[3] See, e.g., U.S. Internet Service Provider Association, Electronic Evidence Compliance—A Guide for Internet Service Providers, 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).

[4] See 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 ("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 ….") (emphasis added).

retroactive attempt to excuse the government's past behavior, rather than a well-considered statutory interpretation:

> Notwithstanding the government's claim that its current explicit reliance on the hybrid theory serves merely to 'dispel' what it allows may have been an initial "lack of clarity on that score," it is apparent that the theory is either an afterthought offered to salvage an application…or alternatively the theory that the government relied on all along but hesitated to expose to judicial scrutiny.

Orenstein Op. II at *22; see also Smith Op. at *16 (government's hybrid theory "amounts to little more than a retrospective assemblage of disparate statutory parts to achieve a desired result."). This conclusion is bolstered by the government's failure to publicly articulate its hybrid argument before now, which is especially notable considering that it claims this combined authority has existed since 1994. See Gov. Br. at 6.

D. 18 U.S.C. § 3117 does not authorize real-time cell-site tracking.

Finally, 18 U.S.C. § 3117 does not independently authorize the use of mobile tracking devices. Rather, it specifies only that "*[i]f* a court is empowered to issue a warrant or other order for the installation of a mobile tracking device" under some other authority, that order can authorize tracking both within and without the issuing court's jurisdiction. See 18 U.S.C. § 3117(a) (emphasis added); see also Bredar Op. at *6 (Section 3117 "articulates no standard for obtaining permission to install and monitor a tracking device."). Therefore, regardless of whether such an order converts a cell phone into a "mobile tracking device," Section 3117 is of no aid to the government.[5]

II. Lacking statutory authority, this Court may only authorize real-time cell-site tracking with a search warrant issued under Rule 41.

As described above, each previous court found the statutory authority cited by the government lacking. That conclusion alone disposes of the government's application, as Judge Orenstein recognized. See Orenstein Op. II at *29. However, Judges Bredar and Smith went further,

---

[5] Of course, the government does not even contend that cell phones are tracking devices. To the contrary, the government contends that all of the arguments of the courts and *Amici* "essentially rely on the argument that the prospective disclosure of cell-site information converts cell phones into 'tracking devices,'" a premise the government claims is incorrect. See Gov. Br. at 18 n.9. This is plainly not the case. Rather, each court's holding that cell-site orders convert cell phones into "tracking devices," see Smith Op. at *10-11, Orenstein Op. II at *12-14, and Bredar Op. at *6, is simply another reason – in addition to Section 2703's limitation to historic records – to find that Congress did not intend for Section 2703(d) to authorize orders for real-time location surveillance. See Orenstein Op. II at *13 (Section 2703's inapplicability to prospective surveillance is "a second and independent reason," beyond the "tracking device" holding, to reject the government's reliance on that section).

finding that a probable cause-based search warrant under Federal Rule of Criminal Procedure 41 could constitutionally authorize the requested surveillance. See Smith Op. at *16; Bredar Op. at *1.

Amici agree that, absent statutory authorization, Rule 41 is the only remaining authority under which this Court could possibly issue a cell-site order. However, *Amicus* EFF humbly disagrees with the finding that a warrant issued under Rule 41, without more, would satisfy the Fourth Amendment.

III. Only a Rule 41 search warrant that also meets the core requirements of the Wiretap Act will satisfy the Fourth Amendment.

None of the three courts found it necessary to decide in their published opinions whether the requested cell-site orders implicated the Fourth Amendment. See Smith Op. at *9, Orenstein Op. II at *27-28, and Bredar Op. at *4 n.7. Each judge did however express doubts about the government's assertion that Fourth Amendment protections did not apply. As Judge Bredar explained: "[t]hose who choose to carry a cell phone…cannot reasonably be deemed to have consented to the tracking of their movement by the government." Bredar Op. at *7 n.12; see also id. at *4 n.8 (distinguishing cell-site data from the phone numbers at issue in Smith v. Maryland, 442 U.S. 735 (1979)); Smith Op. *8-9 (same), Orenstein Op. II *27-29 (same).

Tracking a cell phone invades an individual's privacy interests in ways that go beyond a typical search and instead mirror the Supreme Court's concerns about eavesdropping, as expressed in Berger v. New York: the surveillance is ongoing, surreptitious, and lacks particularity.[6] Admittedly, surveillance conducted using a typical tracking device, which may be authorized by a regular search warrant, shares these qualities. However, and put simply, a cell phone is nothing like a tracking device attached to a multi-gallon tank of chemicals[7] or the bumper of a car. A cell phone will be carried and used, and therefore tracked, from the boardroom to the bedroom, in locales far more varied and more private than those larger items. A mere warrant, without more, is insufficient to prevent unreasonable searches when it comes to such intrusive surveillance.

Considering the constitutional interests at stake, and the lack of guidance from Congress or higher courts, this Court should do what the Appeals Courts have uniformly done when similarly faced with new and invasive modes of electronic surveillance: require that the

---

[6] See 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).

[7] See United States v. Knotts, 460 U.S. 276 (1983) (evaluating whether monitoring of tracking device attached to large drum of chemicals in suspect's possession violated Fourth Amendment) and United States v. Karo, 468 U.S. 705 (1984) (same).

surveillance satisfy the core requirements of 18 U.S.C. §§ 2510 et seq., otherwise known as the "Wiretap Act." See United States v. Biasucci, 786 F.2d 504 (2d. Cir. 1986), cert. denied, 479 U.S. 827 (1986) (holding that video surveillance must meet core requirements of Wiretap Act to satisfy Fourth Amendment); United States v. Torres, 751 F.2d 875 (7th Cir. 1984), cert. denied, 470 U.S. 1087 (1985) (same); United States v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987) (same); United States v. Mesa-Rincon, 911 F.2d 1433 (10th Cir. 1990) (same); and United States v. Koyomejian, 970 F. 2d 536, cert. denied, 506 U.S. 1005 (1992) (holding that Wiretap Act literally applies to video surveillance because of Congress' broad intent); see generally Freiwald, 56 ALA. L. REV. at 72.

In this circuit, the Appeals Court has required that a warrant for video surveillance meet four core requirements from the Wiretap Act:

> (1) the judge issuing the warrant must find 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," 18 U.S.C. § 2518(3)(c); (2) the warrant must contain "a particular description of the type of [information] sought to be intercepted, and a statement of the particular offense to which it relates," id. § 2518(4)(c); (3) the warrant must not allow the period of interception to be "longer than is necessary to achieve the objective of the authorization, []or in any event longer than thirty days" (though extensions are possible), id. § 2518(5); and (4) the warrant must require that the interception "be conducted in such a way as to minimize the interception of [information] not otherwise subject to interception under [Title III]," id.

U.S. v. Biasucci, 786 F.2d at 510. Congress has 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. Congress designed the Wiretap Act to cure the constitutional defects identified by the Supreme Court in Berger, and its exacting requirements "d[o] not suffer from the infirmities that the Court found fatal" to the eavesdropping statute at issue in that case. United States v. Tortorello, 480 F.2d 764, 775 (2d Cir. 1973), cert. denied, 414 U.S. 866 (1973).

Applying the Wiretap Act's high standards of particularity and minimization to the "location wiretap" that the government seeks here is the only option available to this Court, absent guidance from higher courts, which will absolutely ensure that Fourth Amendment rights will not be violated. Furthermore, such a holding may be the only one that will motivate the government to seek appellate review and prompt the needed guidance.

IV. Conclusion

For the foregoing reasons, *Amici* urge this court to deny any application seeking real-time or prospective cell-site information that is not supported by probable cause, and *Amicus* EFF

further recommends that cell-site surveillance be authorized only under terms consistent with the core requirements of the Wiretap Act.

Respectfully submitted,

YUANCHUNG LEE
Assistant Federal Defender
Tel.: (212) 417-8742

WENDY SELTZER (WS-4188)
Attorneys for EFF
250 Joralemon Street
Brooklyn, NY 11201
Telephone: (718) 780-7961
Facsimile: (718) 780-0394
wendy@seltzer.org

cc: Thomas G.A. Brown, Esq.
Assistant United States Attorney
United States Attorney's Office
Southern District of New York
One St. Andrew's Plaza
New York, NY 10007
(BY HAND)

cc: Honorable Gabriel W. Gorenstein
United States Magistrate Judge
Southern District of New York
500 Pearl Street
New York, NY 10007
(BY HAND)