November 4, 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, NY 11722-4454

RE: *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:

As this Court has recognized, "Wisdom too often never comes, and so one ought not to reject it merely because it comes too late." In that spirit, amicus Electronic Frontier Foundation ("EFF") respectfully submits this letter.

Upon reviewing the Court's exhaustively well-reasoned second decision in this case,[1] and especially the Court's detailed discussion of the Application made by the government, EFF is concerned that another of the government's requests—in addition to the denied phone-tracking request—was not authorized by statute.

Specifically, EFF humbly submits that 18 U.S.C. § 2703 does not authorize an order imposing a continuing obligation on all "relevant service providers… to provide subscriber information about [all] numbers obtained from the use of… pen/trap devices" upon oral or written demand by relevant law enforcement officials.[2] Such an ongoing Section 2703(d) order, presumably lasting for the duration of the related pen-trap order issued under 18 U.S.C. § 3123, is a statutory chimera as unsupported as the government's "hybrid" argument for cell phone tracking.

As this Court has already found in the context of the government's cell phone tracking request, Congress did not intend Section 2703(d) to authorize orders that impose

---

[1] *In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information*, ___ F.Supp.2d ___, 2005 WL 2739208 (E.D.N.Y. Oct. 24, 2005).

[2] *Id*. at *2-3.

continuing obligations to produce information over a period of time.[3] This conclusion is supported by the fact that the Stored Communications Act of which Section 2703 is a part, unlike the Wiretap Act and the Pen/Trap statute, "makes no mention of surveillance periods, extensions, periodic reporting or sealing."[4]

Furthermore, Section 2703 provides that "a governmental entity may require *a* provider of electronic communications service…to disclose *a* record or other information pertaining to *a* subscriber or customer of such service…*only* when the government… obtains a court order *for such disclosure* under subsection (d) of this section." 18 U.S.C. § 2703(c) (emphasis added). This language clearly contemplates orders that require disclosure of particular records regarding particular customers of particular providers, not general orders that the government can use on its own discretion to continuously demand unspecified records about unspecified people from unspecified providers, for the entire duration of a related pen-trap surveillance.

If the government seeks to obtain subscriber information related to phone numbers captured by pen-trap surveillance, it must proceed in a manner consistent with the surveillance statutes' plain language and structure. Specifically, the government may: (1) begin collecting phone numbers using a pen-trap device installed pursuant to an order issued under 18 U.S.C. § 3123; (2) issue letters under 18 U.S.C. § 2703(f) to the relevant service providers as phone numbers are collected, demanding that the corresponding subscriber information be preserved; and then (3) apply for Section 2703(d) orders demanding disclosure of the preserved subscriber information, whether periodically during the pen-trap surveillance or in a batch at the end.

This procedure would provide relevant subscriber information to investigators in a timely manner, without handing investigators a blank-check order that fails to specify the subscriber information sought or the provider who must disclose it. It would also ensure that the government is strictly held to Section 2703(d)'s requirements, by forcing the government to satisfy the provision's "specific and articulable facts" standard each time it seeks particular records.[5]

---

[3] *See id.* at *13-14.

[4] *Id*. at *14.

[5] Noting that this Court has found otherwise, *see id*. at *3-4, EFF is humbly skeptical that the government would ever be able to provide specific and articulable facts giving reasonable grounds to believe that the identity of *every* person that may call or be called from the Subject Telephone during the *entire* duration of anticipated surveillance will be "relevant and material" to the investigation.

The Stored Communications Act simply does not authorize open-ended or "roving" orders that are enforced based on the government's oral or written representations of its pen-trap results.[6] Indeed, such orders would leave the government in a dangerously unchecked position to obtain subscriber information for any telephone number without court oversight or approval.

Since the Court has already issued the Section 2703(d) order at hand, and the pen-trap order it supplemented has presumably expired, the issue may be moot in this particular case. However, as an officer of the Court, EFF considers itself duty-bound to share its concern and hopefully aid this Court in its future consideration of similar requests. If the Court does ever find occasion to rule on the propriety of such requests in the future, EFF respectfully encourages this Court to publish its decision.

Respectfully submitted,

By: ________________________________

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

[6] By contrast, the Wiretap Act explicitly provides for so-called "roving" wiretap orders that authorize the surveillance of unspecified facilities, subject to specific procedural safeguards. *See* 18 U.S.C. § 2518(11-12).