

April 29, 2009

VIA U.S. MAIL, EMAIL (senator_leahy@leahy.senate.gov),
AND FACSIMILE (202.224.3479)

Senator Patrick J. Leahy
Chairman, Senate Committee on the Judiciary
433 Russell Senate Office Building
Washington, DC 20510

Re: FBI Reporting Concerning Pen Register/Trap and Trace Statistics

Dear Chairman Leahy,

The release this week of the annual Wiretap Report from the Administrative Office of the United States Courts is an important reminder of good accountability procedures for electronic surveillance authority. As required in the original 1968 Act that allowed wiretapping in the United States, this report provides detailed information about the use of wiretaps -- the offense(s) under investigation, the location of the intercept, the cost of the surveillance, and the number of arrests, trials, convictions that directly result from the surveillance, as well as whether encryption prevented law enforcement officials from obtaining the plain text of communications intercepted pursuant to the court orders.¹ For many years, the Electronic Privacy Information Center ("EPIC") has made good use of this annual Wiretap Report to understand and assess the use of the government's electronic surveillance authority and we have routinely posted this information on our web site so that it is widely available to the public.² Whatever one's views may be of the appropriate scope of electronic surveillance, the availability of objective data, routinely made available to the Congress and to the public, helps to promote government accountability and to ensure better public policy.

By way of contrast, the lack of transparency concerning law enforcement's use of "pen register" and "trap and trace" surveillance devices is a matter of great concern. Federal law requires the Attorney General to report to Congress on the Department of Justice's ("DOJ's") use of these devices.³ Yet the DOJ, between 2000 and 2008, did not make public these reports, and has been delinquent in its reporting to lawmakers. Surveillance experts have observed that the DOJ's lack of transparency frustrates oversight and creates "blank spaces on the map of telecommunications surveillance law."⁴

¹ 18 U.S.C. § 2519(3) (2009).

² "EPIC Wiretap Pages," <http://www.epic.org/privacy/wiretap/> (Last visited Apr. 29, 2009).

³ 18 U.S.C. § 3126 (2009).

⁴ Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. Chi. L. Rev. 287, 288 (2008), *available*

The DOJ's reporting delinquency appears to run afoul of statutory reporting requirements that you sponsored and worked to pass in 1999-2000.⁵ In addition to the DOJ's failure to comply with statutory requirements, we have reason to believe that the reports that the DOJ has released significantly under-report the use of pen register and trap and trace surveillance.

We encourage you to ask the Attorney General's office for greater transparency and public disclosure concerning pen register and trap and trace surveillance. This might be accomplished by requiring the DOJ to submit the annual pen register reports to the Administrative Office of the U.S. Courts, which has a proven track record of reliably collecting and publicly disseminating similar statistics regarding wiretap orders. We further ask you to investigate the accuracy of the DOJ's reporting.

"Pen Register" and "Trap and Trace" Devices

Law enforcement agencies use pen register and trap and trace devices to conduct covert surveillance. Pen registers record outgoing non-content information regarding telephone calls and Internet communications.⁶ Non-content information includes telephone numbers dialed and the length of calls, as well as the identities of an email message's sender and recipient.⁷ Trap and trace devices capture the same information concerning incoming communications.⁸

The DOJ Is Required to Report Pen Register and Trap and Trace Data to Congress

Law enforcement agents are not required to obtain search warrants before employing pen registers or trap and trace devices.⁹ Therefore, complying with public reporting requirements is critical. The Electronic Communications Privacy Act of 1986 requires the Attorney General to "annually report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice."¹⁰ In 1999, you sponsored the "Continued Reporting of Intercepted Wire, Oral, and Electronic Communications Act" (S.1769). Enacted on May 2, 2000, the law expanded the information that must be included in the reports.¹¹ The reports must include:

- (1) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;
- (2) the offense specified in the order or application, or extension of an order;

at <http://www.paulschwartz.net/pdf/12%20Schwartz%20Final%202.19.pdf>.

⁵ S. 1769, 106th Cong. (2000) (enacted).

⁶ 18 U.S.C. § 3127 (2009).

⁷ See 18 U.S.C. § 3121(c) (2009); *In re United States for Order for Disclosure of Telecommunications Records*, 405 F. Supp. 2d 435, 438 (S.D.N.Y. 2005).

⁸ *In re United States for Order Authorizing the Use of a Pen Register & Trap*, 396 F. Supp. 2d 45, 48 (D. Mass. 2005).

⁹ *Smith v. Maryland*, 442 U.S. 735, 745 (1979).

¹⁰ 18 U.S.C. § 3126 (2009).

¹¹ S.1769, A bill to continue reporting requirements of section 2519 of title 18, United States Code, beyond December 21, 1999, and for other purposes, <http://www.thomas.gov/cgi-bin/bdquery/z?d106:SN01769:@@L&summ2=m&> (last visited April 3, 2009).

- (3) the number of investigations involved;
- (4) the number and nature of the facilities affected; and
- (5) the identity, including district, of the applying investigative or law enforcement agency making the application and the person authorizing the order.

The reporting requirements are clearly intended to promote transparency and enhance Congress's oversight role. But the requirements have yet to achieve these goals. As Professor Paul M. Schwartz observes, "Pen Register Act reports are not publicly available and generally disappear into a congressional vacuum."¹² This contrasts with reporting of federal wiretaps, which the Administrative Office of the U.S. Courts makes public annually, providing important information to the American public about the use of electronic surveillance authority in the United States.¹³

The DOJ does not publicly disclose pen register reports as a matter of course. As a result, few reports are available to the public. The documents that have been made public were obtained informally from the DOJ, or through Freedom of Information Act requests filed by public interest groups.¹⁴

The DOJ Has Not Complied with Its Obligations

The Electronic Communications Privacy Act requires the Attorney General to "annually report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice."¹⁵ However, between 1999 and 2003, the Department of Justice failed to comply with this requirement. Instead, 1999-2003 data was provided to Congress in a single "document dump," which submitted five years of reports in November 2004.¹⁶ In addition, when the 1999-2003 reports were finally provided to Congress, the documents failed to include all of the information that the Pen Register Act requires to be shared with lawmakers.¹⁷ The documents do not detail the offenses for which the pen register and trap and trace orders were obtained, as required by 18 U.S.C. § 3126(2).¹⁸ Furthermore, the documents do not identify the district or branch office of the agencies that submitted the pen register requests, information required by 18 U.S.C. § 3126(8).

More troubling, there is no indication that the DOJ provided annual pen register reports to Congress for 2004, 2005, 2006, 2007, or 2008.¹⁹ This failure would demonstrate ongoing, repeated breaches of the DOJ's statutory obligations to inform the public and the Congress about

¹² Schwartz at 296.

¹³ See 18 U.S.C. § 2519(3) (2009); Wiretap Report, U.S. Courts, <http://www.uscourts.gov/library/wiretap.html> (last visited April 29, 2009).

¹⁴ Reports are only available covering the years 1999-2003. These reports were first obtained by Professor Patricia Bellia, who "[obtained] the official reports to Congress ... from the DOJ's Office of Legislative Affairs." See Schwartz at 296.

¹⁵ 18 U.S.C. § 3126 (2009).

¹⁶ Schwartz at 297.

¹⁷ *Id.*

¹⁸ Letter from William Moschella, Assistant Attorney General, to Senator Patrick J. Leahy, *et al.*, Nov. 3, 2004 available at <http://www.paulschwartz.net/penregister-report.pdf>.

¹⁹ Schwartz at 297.

the use of electronic surveillance authority.

The Reports May Not Be Accurate

The DOJ's pen register reports for 1999-2003 also call into question the accuracy of the reported data, particularly concerning the use of "hybrid" orders for cellular location information. The 2000 report states that the FBI requested 2,888 pen registers and 1,656 trap and trace devices. The 2001 report states that the FBI requested 2,350 pen registers and 1,283 trap and trace devices. The 2002 report states that the FBI requested 1,703 pen registers and 991 trap and trace devices.

Law enforcement agents use "hybrid" orders for cellular location information. Hybrid orders seek to determine a suspect's past and future location based on non-content data transmitted by the suspect's cellular phone. The government has engaged in this type of surveillance by invoking a combination of authorities under the Pen Register Act and the Stored Communications Act.²⁰ Because they involve the use of pen registers, hybrid orders should be included in the DOJ's annual reports to Congress. Yet publicly available information calls into question the accuracy of the DOJ's reporting. Law enforcement officials often seek the assistance of wireless service providers to implement hybrid order surveillance. At a recent Harvard Law School event, a telecommunications industry lawyer revealed that the major US wireless carriers each receive approximately 100 requests per week for location information.²¹ That is, the four major carriers receive roughly 20,000 requests for customer location information per year. Even if a majority of these requests come from local and state law enforcement entities, these location requests would amount to double the number of reported pen registers per year.

EPIC's Request

We request that you ask the Attorney General to make public pen register and trap and trace reports from 2004 through the present, and to publicly disclose all future reports as a matter of course. This might be accomplished by requiring the DOJ to submit the annual pen register reports to the Administrative Office of the U.S. Courts, which has a proven track record of reliably collecting and publicly disseminating similar statistics regarding wiretap orders. This statistical data could also be made available in web 2.0 compatible formats that would enable more extensive analysis, furthering the President's goal of enabling the use of new technology for a more informed public.²² Furthermore, we ask you to investigate the DOJ's reporting of "hybrid orders" used to request cellular location information.

²⁰ See *In re United States for Order for Disclosure of Telecommunications Records*, 405 F. Supp. 2d 435, 443-49 (S.D.N.Y. 2005); but see *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747 (S.D. Tex. 2005) (denying government request under "hybrid theory"), available at: http://www.txs.uscourts.gov/district/judges/sws/05MJ557_Cell_site_opinion.pdf.

²¹ Speech by Al Gidari at Berkman Center for Internet and Society, video available at: <http://cyber.law.harvard.edu/interactive/events/luncheons/2009/03/gidari>.

²² Transparency and Open Government, Memorandum for the Heads of Executive Departments and Agencies, 74 Fed. Reg. 4685 (Jan. 21, 2009) (stating "Executive departments and agencies should harness new technologies to put information about their operations and decisions online and readily available to the public.").

Thank you for your attention to this issue. We would be pleased to provide any other information the Committee may require.

Sincerely,

Marc Rotenberg
EPIC President

John Verdi
EPIC Counsel

Christopher Soghoian
Student Fellow
Berkman Center for Internet & Society
Harvard University

cc: Glenn A. Fine, U.S. Dep't of Justice, Inspector General