Electronic Frontier Foundation
Protecting Rights and Promoting Freedom on the Electronic Frontier

January 13, 2005

VIA FEDERAL EXPRESS OVERNIGHT DELIVERY

David M. Hardy, Chief
Record/Information Dissemination Section
Records Management Division
Federal Bureau of Investigation
Department of Justice
935 Pennsylvania Avenue, N.W.
Washington, DC 20535-0001

Thomas J. McIntyre, Chief
FOIA/PA Unit
Criminal Division
Department of Justice
Suite 1127, Keeney Building
Washington, DC 20530-000

Melanie Ann Pustay, Deputy Director
Office of Information and Privacy
Department of Justice
Suite 570, Flag Building
Washington, DC 20530-0001

Marie A. O'Rourke, Assistant Director
FOIA/Privacy Unit
Executive Office for United States Attorneys
Department of Justice
Room 7300, 600 E Street, N.W.
Washington, DC 20530-0001

RE: FREEDOM OF INFORMATION ACT REQUEST

Dear Freedom of Information Officers:

This letter constitutes a request for agency records under the Freedom of Information Act, 5 U.S.C. § 552 ("FOIA"). It is submitted on behalf of the Electronic Frontier Foundation ("EFF").

The scope of the federal government's legal authority and technical ability to conduct electronic surveillance has been a matter of great controversy in the wake of the USA

454 Shotwell Street · San Francisco, CA 94110 USA
+1 415 436 9333 +1 415 436 9993 www.eff.org info@eff.org

PATRIOT Act ("PATRIOT").[1] The refusal of the Department of Justice ("DOJ") to publicly state its interpretation of PATRIOT provisions regarding electronic surveillance has left the public crucially uninformed about how the executive branch is using the expanded surveillance authority granted by Congress in the wake of 9/11.

In particular, it is unclear to the public and to privacy advocates such as EFF what types of information regarding Internet communications may or may not be gathered by law enforcement agents using "pen registers" or "trap and trace devices" as defined by 18 U.S.C. § 3127(3) and (4) (collectively and alternatively, "pen-trap devices"), pursuant to an application under 18 U.S.C. § 3122 ("pen-trap application") for an order issued under 18 U.S.C. § 3123 ("pen-trap order").[2] The pen-trap definitions at § 3127(3) and (4) were substantially expanded by PATRIOT § 216. Yet the DOJ's interpretation of those definitions in the context of Internet communications--whether before or after PATRIOT's amendments--is a mystery to the public.

For example, it is unclear whether the DOJ considers a web address or Uniform Resource Locater ("URL") to be the content[3] of an electronic communication,[4] interception of which requires a wiretap order based on probable cause, or non-content "dialing, routing, addressing or signaling information"[5] ("DRAS information") that may be collected with a pen-trap order based only on a certification of relevance.

Although Internet users reasonably expect that their online reading habits are private, the DOJ will not confirm whether it collects or believes itself authorized to collect URLs using pen-trap devices. The DOJ has refused to answer the public's very simple question: "Can the government see what I'm reading on the web without having to show probable cause?" Yet the public's interest in an answer to that question, which implicates the most profound constitutional rights, is inestimable.

The public has a right to know where the government draws the line between information that can and cannot be collected by a pen-trap device and to know whether the devices used are adequately protective of privacy. EFF therefore seeks disclosure of the

---

[1] *See* "The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act," Pub. L. No. 107-56 (2001).

[2] Records regarding use of pen registers and trap and trace devices authorized under the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq.*, are outside the scope of this request.

[3] "'Contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2511(8).

[4] "'Electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2511(12).

[5] As used in the definitions of "pen register" and "trap and trace device," *see* 18 U.S.C. § 3127.

following agency records, whether in whole or in part and whether in paper or electronic form, and including all records in your possession regardless of the originating agency:

> All records, including blank forms, prepared or collected by the DOJ, the Federal Bureau of Investigation ("FBI"), or any U.S. Attorney's Office in connection with, in preparation for, or in response to any inquiry made to the Computer Crime and Intellectual Property Section ("CCIPS") of the DOJ's Criminal Division by any U.S. Attorney or other DOJ or FBI employee regarding the use of pen-trap devices to monitor electronic communications or Internet-based wire communications[6] (i.e., "Voice-over-Internet-Protocol" or "VOIP" communications). This request encompasses inquiries made at any time before or after PATRIOT's enactment, and includes but is not limited to records concerning "prior consultations" with CCIPS made in accordance with the DOJ's U.S. Attorneys' Manual.[7]

Relevant inquiries may include but are not limited to the following:

a) What particular types of information constitute DRAS information that may be collected via a pen-trap device when monitoring electronic or VOIP communications, and why? (E.g., "Are URLs dialing, routing, addressing or signaling information that can be collected using a pen register or trap and trace device, as those are defined by 18 U.S.C. § 3127?")

b) What particular types of information constitute content that may not be collected via a pen-trap device when monitoring electronic or VOIP communications, and why?[8] (E.g., "Are email subject lines 'content' as defined by 18 U.S.C. § 2511(8)?")

---

[6] "'Wire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce." 18 U.S.C. § 2511(1).

[7] *See United States Attorneys' Manual* ("USAM") at 9-7500, *"Prior Consultation with the Computer Crime and Intellectual Property Section of the Criminal Division (CCIPS) for Applications for Pen Register and Trap and Trace Orders Capable of Collecting Uniform Resource Locators (URLs),"* available at <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/title9.htm>.

[8] DOJ and FBI employees have repeatedly been instructed to address such inquiries to CCIPS:

- "Any questions about what constitutes 'content' must be coordinated with Main Justice.... [S]uch questions should be addressed...to...the Computer Crime and Intellectual Property Section in the computer context (202-514-1026)." *Deputy*

c) What particular devices constitute pen-trap devices in the context of electronic or VOIP communications, and why?[9] (E.g., "Is (x) software or (y) hardware configured in (z) manner a pen register or trap and trace device, as those are defined by 18 U.S.C. § 3127?")

This request includes but is not limited to inquiries about whether the following types of information constitute content or DRAS information:

- URLs,
- IP addresses,
- Email addresses,
  Email subject lines,
- Transport protocols used,
- Ports accessed,
- Communication size in bytes,
- Time and date stamps, or
  Any combination of the above.

2. All policy directives or guidance issued before or after PATRIOT's effective date to any U.S. Attorneys or other DOJ or FBI employees regarding the potential or actual use of pen-trap devices to monitor electronic or VOIP communications, including but not limited to any policy directives or guidance relevant to the inquiries cited above.

3. All policy directives or guidance issued to any U.S. Attorneys or other DOJ or FBI employees regarding what constitutes "technology reasonably available to [a government agency] that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information

---

Attorney General Larry Thompson's May 24, 2002 Memorandum on "Avoiding Collection and Investigative Use of 'Content' in the Operation of Pen Registers and Trap and Trace Devices" ("Thompson Overcollection Memo"), formerly available at <http://www.house.gov/judiciary/attachD.PDF>.

- "Agents and prosecutors with questions about whether a particular type of information constitutes content should contact...the Computer Crime and Intellectual Property Section in the computer context (202-514-1026)." *CCIPS' "Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA PATRIOT Act of 2001" ("CCIPS Field Guidance")*, available at <http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm>.

[9] DOJ and FBI employees have been instructed to address such inquiries to CCIPS. *See CCIPS' "Searching and Seizing Computers and Related Electronic Evidence Issues,"* XXX(C)(1), available at <http://www.usdoj.gov/criminal/cybercrime/searching.html> ("Prosecutors or agents may have questions about whether particular devices constitute pen registers or trap and trace devices, and they should direct any such questions to the Computer Crime and Intellectual Property Section at (202) 514-1026....")

utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications" under 18 U.S.C. § 3121(c).

4. All records, including blank forms, prepared or collected by the DOJ, the FBI, or any U.S. Attorney's Office in connection with any and all instances of "overcollection" ("the collection of 'content' in the use of pen registers or trap and trace devices under chapter 206,"[10] i.e., under 18 U.S.C. § 3121 *et seq.*).

5 All policy directives or guidance issued to any U.S. Attorneys or other DOJ or FBI employees regarding DOJ or FBI policy on the avoidance of overcollection and the handling of overcollected content.

6. All records, including blank forms, prepared or collected by the DOJ, the FBI or any U.S. Attorney's Office in connection with any potential or actual use of overcollected content, whether for an affirmative investigative purpose or otherwise.[11]

7. All records collected and prepared in accordance with 18 U.S.C. § 3123(a)(3)(A), "where the law enforcement agency implementing an ex parte order under this subsection [did so] by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public."

8 All annual reports submitted to Congress as required by 18 U.S.C. § 3126,[12] from January 1st, 1999 to the present, and all records prepared or collected in order to prepare or complete those reports or any future report.

9. Any other report or testimony to Congress made by the DOJ, the FBI, or any U.S. Attorney's Office, whether before or after PATRIOT's enactment, regarding the actual or potential use of pen-trap devices to monitor electronic or VOIP communications, and all records prepared or collected in order to prepare or complete any past or future report or testimony.

10. All court decisions and legal pleadings filed by any party regarding any pen-trap application seeking or any pen-trap order authorizing the collection of information about electronic or VOIP communications, whether before or after PATRIOT's enactment. This request includes but is not limited to all decisions and pleadings in every case where a pen-trap application sought or a

---

[10] *Thompson Overcollection Memo.*

[11] "[I]t is the policy of this Department that [overcollected] content may not be used for any affirmative investigative purpose, except in a rare case in order to prevent an immediate danger of death, serious physical injury, or harm to national security." *Id.*

[12] "The Attorney General shall 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...." 18 U.S.C. § 3126.

pen-trap order authorized the collection of information on a computer network, and every case where a private litigant challenged such a pen-trap order. [13]

1. Any agency records containing the following information, for the years 1990 to the present:

   a) The number of pen-trap orders applied for, issued, and/or implemented, where law enforcement requested the installation or use of its own pen-trap device to monitor electronic or VOIP communications, whether on the packet-switched data network of a provider of electronic communication service to the public or otherwise.[14]

   b) The number of pen-trap orders applied for, issued, and/or implemented to collect the URLs visited by a surveillance target, including the number of those to collect complete URLs, and the number of those to collect only a specific portion of URLs (e.g., while <http://www.eff.org/privacy/> is a complete URL pointing to a particular web page, <http://www.eff.org> reveals only the second-level domain of a particular web site).

   c) The number of pen-trap orders applied for, issued, and/or implemented to collect the IP addresses visited by a surveillance target, including the number of IP addresses collected.

   d) The number of pen-trap orders applied for, issued, and/or implemented to collect the IP addresses visited by a surveillance target, where the IP addresses could be readily translated into URLs or portions of URLs.[15]

   e) The number of pen-trap orders applied for, issued, and/or implemented to collect "tracing information indicating the source of requests to view a particular URL,"[16] including the number of pen-trap orders applied for, issued, and/or implemented for each particular type of tracing information collected, and the number of URLs that were monitored.

---

[13] "Numerous courts across the country have applied the [pre-PATRIOT] pen/trap statute to communications on computer networks," and "certain private litigants have challenged the application of the pen/trap statute to such electronic communications based on the statute's telephone specific language." *CCIPS Field Guidance. See also, e.g., In re United States of America*, Cr. No. 99-2713M (C.D. Cal. Feb. 4, 2000) (McMahon, Mag. J.) (unpublished opinion, available at <http://www.epic.org/privacy/carnivore/cd_cal_order.html>) (applying pre-PATRIOT pen-trap statute to Internet communications).

[14] *See* 18 U.S.C. § 3123(a)(3)(A).

[15] Prior consultation with CCIPS is not required for "applications for pen register orders that would merely authorize collection of Internet Protocol (IP) addresses, even if such IP addresses can be readily translated into URLs or portions of URLs." *USAM* at 9-7.500.

[16] *Id.*

f) The number of pen-trap orders applied for, issued, and/or implemented to collect tracing information indicating the source of requests to access a particular IP address, including the number of pen-trap orders applied for, issued, and/or implemented for each particular type of tracing information collected, the number of IP addresses that were monitored, the number of those IP addresses that hosted more than one second-level domain or web site, and the number of second-level domains or web sites affected.

g) The particular types of devices, including hardware and software and whether provided by the government or a third-party, approved by the DOJ, FBI, or any U.S. Attorney's Office for use as pen-trap devices to collect information regarding electronic or VOIP communications, and the number of pen-trap applications that sought or pen-trap orders that authorized each particular type of device's use for collection of such information.

h) The number and nature of facilities where a pen-trap device was used pursuant to a pen-trap order to collect information regarding electronic or VOIP communications. In the context of telephones, the "facility" would be the particular phone line that was monitored; in the context of the Internet, facilities would include, e.g., particular email addresses, URLs, or VOIP telephone numbers that were monitored.

i) The number of individual persons whose communications were monitored as a result of each pen-trap order to collect information regarding electronic or VOIP communications, and the total number of such individuals monitored for each year, including individuals not targeted by an order whose communications were incidentally monitored.

j) The number of individual communications monitored as a result of each pen-trap order to collect information regarding electronic or VOIP communications, and the total number of such communications monitored for each year, including the communications of individuals not targeted by an order whose communications were incidentally monitored.

Waiver of Processing Fees

The requester qualifies as a "representative of the news media," and fees associated with the processing of this request must therefore be "limited to reasonable standard charges for document duplication." 5 U.S.C. § 552(a)(4)(A)(ii)(II). The requester is a news media organization that "gathers information of potential interest to a segment of the public" and "uses it editorial skills to turn raw materials into a distinct work, and distributes them to an audience." *National Security Archive v. Department of Defense*, 880 F.2d 1381, 1387 (D.C. Cir. 1989).

EFF is a non-profit, member-supported civil liberties organization, advocating for the protection of civil rights and free expression in the digital world. In that role EFF

publishes educational and advocacy materials for its 13,000 members and the public, via a weekly email newsletter and <http://www.eff.org>, one of the most linked-to web sites on the Internet.

The records requested are not sought for commercial use, and the requester plans to disseminate the information disclosed as a result of this FOIA request through the channels described above.

Waiver of Duplication Costs

Additionally, we request a fee waiver for duplication costs because disclosure of this information is in the public interest. The information EFF seeks is likely to contribute significantly to the public understanding of government activity. EFF is a nonprofit 501(c)(3) research and education organization working to increase citizen participation in governance issues. The requester is making this request specifically to further the public's understanding of the government's use of its surveillance authority within the United States.

Although the DOJ has consistently praised PATRIOT as a key tool in the fight against terror that does not pose a threat to civil liberties, *see, e.g.*, <http://www.lifeandliberty.gov>, the DOJ has failed to adequately inform the public about its use of PATRIOT powers, *see, e.g.*, Adam Clymer, "Justice Dept. Balks at Effort to Study Antiterror Powers," *New York Times* (August 14, 2002). Specifically, while assuring the public that PATRIOT's expansion of pen-trap authority to the Internet "has proven as effective at safeguarding Fourth Amendment values as it has at bringing terrorists to justice,"[17] the DOJ has refused to publicly state whether or not it uses that authority to collect URLs or other content-revealing information without probable cause.

The exact scope of the DOJ's legal authority and technical ability to conduct pen-trap surveillance of Internet communications has been a matter of great public controversy since even before PATRIOT's passage; news articles reflect the strong and continued public interest in the materials EFF seeks in our request. See, e.g.,

- Nick Gillespie, "Penned, Trapped: The Absurd Claim That PATRIOT Increases Your Privacy," *Reason Online* (September 4, 2003) (challenging DOJ's characterization of PATRIOT § 216 as privacy-enhancing; available at <http://www.reason.com/links/links090403.shtml>);

---

[17] *Anti-Terrorism Investigations and the Fourth Amendment after September 11, 2001: Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 108th Cong. 28 (1993) (prepared statement of Viet D. Dinh, Assistant Attorney General for the Office of Legal Policy, Department of Justice). *See also* <http://www.lifeandliberty.gov/subs/add_myths.htm#_Toc65482102> ("[S]ection 216 **enhanced the privacy protections** in the pen-register statute," a statute which provides for "robust oversight" of law enforcement and "ensures that law enforcement will be able to collect non-content information about terrorists' communications...").

- Patricia Cohen, "9/11 Law Means More Snooping? Or Maybe Less?" *New York Times* (September 7, 2002) (reporting on debate over impact of PATRIOT's expansion of pen-trap authority to the Internet);
- Kevin Galvin, "Rights and Wrongs: Why New Law-Enforcement Powers Worry Civil Libertarians," *Seattle Times* (December 6, 2001) (discussing civil libertarians objections to PATRIOT, including its expansion of pen-trap authority);
- Carrie Kirby, "Watchdogs Say Terror Bill Goes Too Far," *San Francisco Chronicle* (October 25, 2001) (noting civil libertarians objections to new surveillance authorities in anti-terror bill, including pen-trap authority);
- Carl Kaplan, "Concern Over Proposed Changes in Internet Surveillance, *New York Times* (September 21, 2001) (reporting on the debate over proposed anti-terror bill's impact on Internet surveillance and discussing the Internet pen-trap controversy);
- John Schwartz, "FBI Makes Case For Net Wiretaps; 'Carnivore' System Faces Fire on Hill," *The Washington Post* (July 25, 2000) (describing controversy over FBI's use of 'Carnivore' to conduct Internet wiretaps and pen-trap surveillance); and
- John Markoff, "Digital-Age Wiretapping Plan By F.B.I. Draws Opposition," *New York Times* (August 11, 1997) (discussing Internet pen-trap surveillance in the context of a debate over the Communications Assistance for Law Enforcement Act).

Law review articles also evidence a continuing controversy over the application of pen-trap authority when applied to the Internet. *Compare, e.g.*, Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 Nw. U. L Rev. 607, 639 (2003) (arguing the privacy benefits of PATRIOT's changes to the pen-trap statute) *with* Laurie Thomas Lee, *The USA PATRIOT Act and Telecommunications: Privacy Under Attack*, 29 Rutgers Computer & Tech. L.J. 371, 394 (2003) (questioning the constitutionality of PATRIOT's changes to the pen-trap statute).

The public interest in the materials EFF seeks is heightened by the fact that many PATRIOT provisions are set to expire at the end of 2005. Both Congress and the public need more information on how PATRIOT powers are currently being used in order to fully debate those provisions' renewal, or to advocate for or against the expiration of additional provisions.

If EFF's request is denied in whole or part, we ask that you justify all deletions by reference to specific exemptions of the FOIA. EFF expects you to release all segregable portions of otherwise exempt material.

We further ask that all responsive records be produced as they are identified and gathered, rather than delaying production until all responsive records are found. EFF is open to negotiating a modification to this request where production of all responsive documents would be unreasonably voluminous. However, EFF reserves the right to appeal a decision to withhold any information or to deny a waiver of fees.

Please also be advised that, by separate letter to Barbara Comstock, Director of Public Affairs for DOJ, we are requesting the expedited processing of this request. Notwithstanding Ms. Comstock's determination, we look forward to your reply within 20 business days, as the statute requires under Section 552(a)(6)(A)(I).

Thank you for your prompt attention to this matter.

Please respond to Kevin Bankston, Attorney and Equal Justice Works/Bruce J. Ennis Fellow, Electronic Frontier Foundation, 454 Shotwell Street, San Francisco, CA 94110, telephone (415) 436-9333, ext. 126.

_____

KEVIN S. BANKSTON
Attorney and Bruce J. Ennis/Equal Justice Works Fellow
Electronic Frontier Foundation

cc: JOSHUA KOLTUN, Counsel for Requester
DLA Piper Rudnick Gray Cary US LLP
333 Market Street, Suite 3200
San Francisco, CA 94105-2150
Direct tel. 415-659-7027
Direct fax. 415-659-7327
Main tel. 415-659-7000
Main fax. 415-659-7300