

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

ELECTRONIC FRONTIER FOUNDATION,)	
)	
Plaintiff,)	
)	
v.)	Civil Action No. 10-cv-4892-DMR
)	
U.S. DEPARTMENT OF JUSTICE,)	
)	
Defendant.)	
)	

DECLARATION OF KRISTIN L. ELLIS

I, Kristin L. Ellis, declare the following to be a true and correct statement of facts:

1. I am a Trial Attorney in the U.S. Department of Justice (DOJ), Criminal Division (CRM) and am currently assigned to the Freedom of Information Act/Privacy Act (FOIA/PA) Unit, a component in the Office of Enforcement Operations (OEO).
2. Among other things, I am responsible for reviewing complaints in lawsuits filed under the Freedom of Information Act (FOIA), 5 U.S.C. §§ 552 *et seq.*, and the Privacy Act (PA), 5 U.S.C. §§ 552 *et seq.*, and providing litigation support and assistance to Assistant United States Attorneys and Department Trial Attorneys who represent the Department's interests in such lawsuits in the United States District Courts. In providing such assistance and support, I review processing files compiled in responding to FOIA/PA requests received by CRM, to determine whether searches for records were properly conducted and whether decisions to withhold or release CRM records were in accordance with the FOIA, PA, and DOJ regulations at 28 C.F.R. §§ 16.1 *et seq.* If searches are incomplete and/or records have not been processed, I

ensure that searches are completed and either process or oversee the processing of responsive records by FOIA/PA staff members. I consult with the Chief of the FOIA/PA Unit, Deputy Chief of the FOIA/PA Unit, and supervisory paralegal specialists as part of my review.

3. Due to the nature of my official duties, I am familiar with the processing of the FOIA request at issue in this litigation. Specifically, in this instance, I reviewed the processing file and records related to Plaintiff's FOIA request; I consulted, and continue to consult, with CRM components and other DOJ agencies possessing responsive records; and I followed-up, and continue to follow up, on pending searches. I also have begun reviewing records located during CRM's searches. The statements that follow are made on the basis of my review of CRM's official files and records, my own personal knowledge, and information I acquired in performing my official duties.

BACKGROUND

4. Plaintiff submitted a FOIA request dated September 28, 2010, to CRM via facsimile. CRM received the request on September 29, 2010. A true and correct copy of the request is attached as Exhibit 1 (FOIA request).

5. Plaintiff requested:

[A]ll agency records created on or after January 1, 2006 (including, but not limited to, electronic records) discussing, concerning, or reflecting:

1. any problems, obstacles or limitations that hamper the DOJ's current ability to conduct surveillance on communications systems or networks including, but not limited to, encrypted services like Blackberry (RIM), social networking sites like Facebook, peer-to-peer messaging services like Skype, etc.;
2. any communications or discussions with the operators of communications systems or networks (including, but not limited to, those providing encrypted communications, social networking, and peer-to-peer messaging services), or with equipment manufacturers

and vendors, concerning technical difficulties the DOJ has encountered in conducting authorized electronic surveillance;

3. any communications or discussions concerning technical difficulties the DOJ has encountered in obtaining assistance from non-U.S.-based operators of communications systems or networks, or with equipment manufacturers and vendors in the conduct of authorized electronic surveillance;
4. any communications or discussions with the operators of communications systems or networks, or with equipment manufacturers and vendors, concerning development and needs related to electronic communications surveillance-enabling technology;
5. any communications or discussions with foreign government representatives or trade groups about trade restrictions or import or export controls related to electronic communications surveillance-enabling technology;
6. any briefings, discussions, or other exchanges between DOJ officials and members of the Senate or House of Representatives concerning implementing a requirement for electronic communications surveillance-enabling technology, including, but not limited to, proposed amendments to the Communications Assistance for Law Enforcement Act (CALEA).

Id. at p. 2.

6. Plaintiff also requested that its request be granted expedited treatment, pursuant to 28 C.F.R. § 16.5(d)(1)(ii), which provides that requests “will be taken out of order and given expedited treatment whenever it is determined that they involve ... an urgency to inform the public about an actual or alleged federal government activity, if made by a person primarily engaged in disseminating information.” See id. at pp. 2-3.

7. Plaintiff averred that expedited treatment was warranted because of “the proposed introduction of legislation that would impose new technical requirements on communications providers,” and because, it posited, the information requested “will help the public and Congress fully participate in [the] ongoing debate over whether to increase – or restrict – the investigative authority of the federal government.” Plaintiff quoted from a *New York Times* article, which

reported that the Obama administration planned to propose “sweeping new regulations for the Internet ... next year.” *Id.* at p. 3; see also Exhibit 2 (a true and correct copy of the referenced *New York Times* article).

8. Upon information and belief, the legislation plaintiff described had not been presented to Congress at the time of plaintiff’s request, nor has it been presented to date.

9. In a letter dated October 4, 2010, CRM acknowledged receipt of the request for information and denied plaintiff’s request for expedited treatment. CRM explained that it was denying the request for expedited processing because “we do not believe that your request for information about legislation that may or may not be proposed to Congress next year satisfies the criteria for expedited processing.” A true and correct copy of this letter is attached as Exhibit 3 (CRM Acknowledgment Letter).

SEARCH AND REVIEW

10. CRM continues to systematically search for information responsive to plaintiff’s request. We initiated searches on October 6, 2010. Agency personnel familiar with the request and with CRM’s various offices initially determined that based on the subject matter of the request, the offices most likely to possess responsive information were: the Computer Crime and Intellectual Property Section (CCIPS); the Office of International Affairs (OIA); the Office of Policy and Legislation (OPL); and OEO’s Electronic Surveillance Unit (ESU). The FOIA/PA Unit sent each office a search request that included a copy of plaintiff’s FOIA request.

11. On November 5, 2010, while CRM’s search for responsive records was on-going, the Government was served with plaintiff’s lawsuit in this matter. CRM learned about the lawsuit on November 10, 2010.

12. Even though CRM did not grant plaintiff's request for expedited treatment of its FOIA request, CRM began treating the request as a priority in November 2010, and is processing the request "as soon as practicable." See 5 U.S.C. § 552(a)(6)(E)(iii). (For instance, on November 5, 2010, when defendants were served, CRM had 134 FOIA/PA requests pending; 92 were older than plaintiff's request.) As shown below, CRM has made significant progress in processing plaintiff's request. As of the date of this declaration, CRM's searches for records responsive to plaintiff's request are near completion and CRM has begun reviewing the search results to determine the responsiveness and releasability of the information we located.

13. On November 12, 2010, I contacted CCIPS, OIA, OPL, and ESU to determine the status and progress of its searches for responsive records. As a result of my contacts, we learned that a wider segment of CRM offices may have information that is potentially responsive to plaintiff's request. . Thereafter, CRM expanded its search for responsive information. On November 17, 2010, all Office of Enforcement Operations (OEO) employees were asked to search for responsive information, and on November 30, 2010, all CRM employees were asked to search for responsive information. (The FOIA/PA Unit is part of OEO. OEO is an office within the Criminal Division.) OEO employees were instructed to report if they located any potentially responsive information by November 26, 2010; all other CRM employees were instructed to report if they located any potentially responsive information by December 10, 2010. Both the November 17th and 30th search requests included copies of plaintiff's FOIA request.

14. To date, all employees who reported that they located potentially responsive information in hard copy, except one, have provided the information to the FOIA/PA Unit. The remaining employee was physically away from the office during the period when the searches were initiated but she is currently conducting her search and anticipates providing any potentially

responsive information she locates before the end of January. The FOIA/PA Unit continues to work with her to complete the search. We currently do not have an exact page count of the hard copy records provided to the FOIA/PA Unit, but we estimate that there are approximately 3750 pages.

15. Employees were also instructed to report to the FOIA/PA Unit whether they believed they might have potentially responsive information in electronic form (*i.e.*, in their e-mail accounts or on their personal network (H:) drives). The FOIA/PA Unit then coordinated with CRM's Information Technology Management (ITM) office, which conducted a global search of most of those employees' unsecured e-mail accounts. (Several employees were sufficiently aware of the extent and location of the potentially responsive information they had in their e-mail accounts/on their H: drives. Accordingly, they conducted their own electronic searches and provided any potentially responsive information they located to the FOIA/PA Unit. These search results are included in the estimate of hard copy records previously discussed.)

16. ITM completed its electronic search of employees' e-mail accounts and provided the FOIA/PA Unit with the results on January 6 and 11, 2011. ITM's search located slightly more than 3000 potentially responsive e-mails, many of which include one or more attachments.

17. The FOIA/PA Unit continues to coordinate with ITM regarding the search of employees' H: drives, as well as a shared network (S:) used by CCIPS. In order to conduct these searches, ITM currently is restoring the last full backup from three servers and anticipates it will take two-to-three weeks to conduct the searches and organize the results once the restoration is complete.

18. Finally, two CRM employees reported to the FOIA/PA Unit that they likely had potentially responsive e-mails in their secured (classified) e-mail accounts. One employee

searched her secured account, located potentially responsive information, and provided it to the FOIA/PA Unit on December 30, 2010. The other employee works on a secured network maintained by a DOJ component other than CRM. After consulting with the component to determine the best way to search the CRM employee's files located on the other component's secured network, we concluded that the employee would need to conduct the search himself. He is currently in the process of doing so, and the FOIA/PA Unit is continuing to work/coordinate with him to complete the search.

19. Although CRM is processing this request as soon as practicable, it is difficult at this time to estimate accurately the amount of time it will take to complete processing. The processing challenges currently identified by CRM include the following:

a. The subject matter of this request is complex and may require consultation with subject matter experts to assist in determining what information is responsive and whether it is exempt. Moreover, because the subject matter of the information here concerns sensitive law enforcement information, an exacting, thorough line-by-line review is necessary to achieve the greatest level of transparency possible while also protecting the Government's legitimate law enforcement interests.

b. Multiple DOJ components, as well as numerous other Federal agencies, have equities in potentially responsive information located by CRM during its searches, which will necessitate many referrals and consultations. In particular, many of the e-mails CRM located during its searches consist of chains involving employees and officials throughout the Department and across the Federal Government. To adequately ensure that all agencies with equities have had a chance to make determinations about

their information, the same e-mail chains may need to be sent to one or more agencies as referrals or for consultation.

c. CRM located classified information that is potentially responsive to this request. The requirements for handling classified information in order to safeguard it necessitate special processing procedures and will increase the review time for this subset of information.

20. Completing the processing of plaintiff's request within 10 days is not feasible. Instead, taking into account the above-described challenges and factoring in available resources, and in an effort to process the request as soon as practicable, CRM anticipates processing a minimum of 400-500 pages of information every thirty days and making interim responses to plaintiff concerning such processing on a monthly basis. CRM further anticipates processing its first interim response on or about April 1, 2011. This is a good faith estimate, based on the currently known volume and nature of the information involved in this request. It may need to be refined or modified as processing continues.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 25th day of January, 2011.



Kristin L. Ellis

09/28/2010 16:01 FAX 4154369993

EFF

001

201000724F



454 Shotwell Street
San Francisco, CA 94110
+1 415 436 9333 (tel)
+1 415 436 9993 (fax)

FAX COVER SHEET

DATE: September 28, 2010
TO: Rena Y. Kim - DoJ
Fax Number: (202) 514-6117
FROM: Jennifer Lynch
RE: Freedom of Information Act Request
Pages sent: 12 including cover page

COMMENTS:

SEP 29 2010

NOTICE This fax is intended for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential, and exempt from disclosure. If you are not the intended recipient or his or her agent, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited and asked to please notify us immediately by telephone. Thank you.

PLEASE CALL IF THERE IS A PROBLEM



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

September 28, 2010

VIA FACSIMILE — (202) 514-6117

Rena Y. Kim, Chief
FOIA/PA Unit
Criminal Division
Department of Justice
Suite 1127, Keeney Building
Washington, DC 20530-0001

RE: Freedom of Information Act Request and
Request for Expedited Processing

Dear Ms. Kim:

This letter constitutes an expedited request under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and is submitted to the Department of Justice Criminal Division (DOJ) on behalf of the Electronic Frontier Foundation (EFF). We make this request as part of EFF's FOIA Litigation for Accountable Government (FLAG) Project, which works to obtain government documents and make them widely available to the public.

Yesterday the *New York Times* reported that officials from the Department of Justice and other federal agencies have been meeting with White House officials to develop proposed statutory language and regulations to "require all services that enable communications — including encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct 'peer to peer' messaging like Skype — to be technically capable of complying if served with a wiretap order." Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, *New York Times* (Sept. 27, 2010).¹ See also Glenn Greenwald, *The Obama Administration's War on Privacy*, *Salon.com* (Sept. 27, 2010);² Kit Eaton, *What a Wiretappable Internet Could Mean for Facebook, Apple, Google, and You*, *Fast Company* (Sept. 27, 2010);³ Lolita C. Baldor, *Report: US Would Make Internet Wiretaps Easier*, *Washington Post* (Sept. 27, 2010);⁴ Ellen Nakashima, *Administration Seeks Ways to Monitor Internet Communications*, *Washington Post* (Sept.

¹ <http://www.nytimes.com/2010/09/27/us/27wiretap.html>.

² http://www.salon.com/news/opinion/glenn_greenwald/2010/09/27/privacy/index.html.

³ <http://www.fastcompany.com/1691505/wiretap-emails-facebook-apple-google>.

⁴ <http://www.washingtonpost.com/wp-dyn/content/article/2010/09/27/AR2010092700719.html>.

27, 2010);⁵ PBS News Hour, *Proposal Could Expand Government's Web Wiretapping Efforts* (Sept. 27, 2010).⁶

We hereby request all agency records created on or after January 1, 2006 (including, but not limited to, electronic records) discussing, concerning, or reflecting:

1. any problems, obstacles or limitations that hamper the DOJ's current ability to conduct surveillance on communications systems or networks including, but not limited to, encrypted services like Blackberry (RIM), social networking sites like Facebook, peer-to-peer messaging services like Skype, etc.;
2. any communications or discussions with the operators of communications systems or networks (including, but not limited to, those providing encrypted communications, social networking, and peer-to-peer messaging services), or with equipment manufacturers and vendors, concerning technical difficulties the DOJ has encountered in conducting authorized electronic surveillance;
3. any communications or discussions concerning technical difficulties the DOJ has encountered in obtaining assistance from non-U.S.-based operators of communications systems or networks, or with equipment manufacturers and vendors in the conduct of authorized electronic surveillance;
4. any communications or discussions with the operators of communications systems or networks, or with equipment manufacturers and vendors, concerning development and needs related to electronic communications surveillance-enabling technology;
5. any communications or discussions with foreign government representatives or trade groups about trade restrictions or import or export controls related to electronic communications surveillance-enabling technology;
6. any briefings, discussions, or other exchanges between DOJ officials and members of the Senate or House of Representatives concerning implementing a requirement for electronic communications surveillance-enabling technology, including, but not limited to, proposed amendments to the Communications Assistance to Law Enforcement Act (CALEA).

Request for Expedited Processing

This request warrants expedited processing because it pertains to information about which there is an "urgency to inform the public about an actual or alleged federal

⁵ <http://www.washingtonpost.com/wp-dyn/content/article/2010/09/27/AR2010092703244.html>.

⁶ http://www.pbs.org/newshour/bb/government_programs/july-dec10/wiretap_09-27.html.

government activity,” and it is “made by a person primarily engaged in disseminating information.” 28 C.F.R. § 16.5(d)(1)(ii). The information we request easily satisfies this standard.

The federal government activity involved here—the proposed introduction of legislation that would impose new technical requirements on communications providers—raises significant issues concerning potential government intrusions into personal affairs, particularly those involving private communications and activities. The *New York Times* article notes that the Obama administration plans to submit the “sweeping new regulations for the Internet . . . next year.” When Congress begins the process of considering the administration’s request for new legislation, its deliberations will constitute the latest chapter in a public debate over anti-terrorism powers, which has been ongoing since late 2001. The information we request will help the public and Congress fully participate in that ongoing debate over whether to increase—or restrict—the investigative authority of the federal government. Delay in processing this FOIA request could inhibit the public’s ability to fully analyze and debate the implications of the legislative changes the administration seeks.

Notably, the need for expeditious disclosure of information concerning Executive branch requests for greater anti-terrorism authorities is not a matter of first impression. In *ACLU v. Dep’t of Justice*, 321 F. Supp. 2d 24 (D.D.C. 2004), the court held that impending congressional consideration of expiring PATRIOT Act provisions created a “compelling” need for information concerning the FBI’s use of its investigative authorities. As such, the court ordered expedited processing of a FOIA request seeking that information. Similarly, in two cases involving FOIA requests to the Office of the Director of National Intelligence, the court found irreparable harm exists where Congress is considering legislation that would amend a surveillance statute (in these cases, FISA) “and the records may enable the public to participate meaningfully in the debate over such pending legislation.” *Elec. Frontier Found. v. Office of the Dir. of Nat’l Intelligence*, 542 F. Supp. 2d 1181, 1187 (N.D. Cal. 2008)(citing *Elec. Frontier Found. v. Office of the Dir. of Nat’l Intelligence*, 2007 U.S. Dist. LEXIS 89585 (Nov. 27, 2007)). Even though the court could not “predict the timing of passage of the legislation” the court granted expedited processing, holding “that delayed disclosure of the requested materials may cause irreparable harm to a vested constitutional interest in ‘the uninhibited, robust, and wide-open debate about matters of public importance that secures an informed citizenry.’” *Id.* (citing *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964)). Likewise, there is an urgency to inform the public about the information we seek here. Therefore, this request clearly meets the standard for expedited processing set forth in DOJ regulations.

Further, as I explain below in support of our request for “news media” treatment, EFF is “primarily engaged in disseminating information.” Indeed, DOJ components have granted previous EFF requests for expedited processing under 28 C.F.R. § 16.5(d)(1)(ii) and have thus acknowledged that the organization is “primarily engaged in disseminating information.” See Letter to David Sobel of EFF, dated October 21, 2009 (attached).

Request for News Media Fee Status

EFF asks that it not be charged search or review fees for this request because EFF qualifies as a “representative of the news media” pursuant to the FOIA and 28 C.F.R. § 16.11(b)(6). In requesting this classification, we note that the Department of Homeland Security (DHS) has recognized that EFF qualifies as a “news media” requester based upon the publication activities set forth below (*see* DHS stipulation attached). In addition, the National Security Agency (NSA) has previously determined that EFF is not only a “news media requester,” but also “primarily engaged in disseminating information” for purposes of expedited processing (*see* attached NSA response to prior EFF FOIA request, in which EFF requested expedited processing because it sought information “urgently needed by an individual primarily engaged in disseminating information in order to inform the public concerning actual or alleged Federal Government activity,” and NSA granted the request). These precedents are particularly important in light of the fact that the U.S. Court of Appeals for the D.C. Circuit has stressed that “different agencies [must not] adopt inconsistent interpretations of the FOIA.” *Al-Fayed v. CIA*, 254 F.3d 300, 307 (D.C. Cir. 2001), quoting *Pub. Citizen Health Research Group v. FDA*, 704 F.2d 1280, 1287 (D.C. Cir. 1983).

EFF is a non-profit public interest organization that works “to protect and enhance our core civil liberties in the digital age.”⁷ One of EFF’s primary objectives is “to educate the press, policymakers and the general public about online civil liberties.”⁸ To accomplish this goal, EFF routinely and systematically disseminates information in several ways.

First, EFF maintains a frequently visited web site, <http://www.eff.org>, which received 43,403,630 hits in June 2007 — an average of 60,282 per hour. The web site reports the latest developments and contains in-depth information about a variety of civil liberties and intellectual property issues.

EFF has regularly published an online newsletter, the EFFector, since 1990. The EFFector currently has more than 77,000 subscribers. A complete archive of past EFFectors is available at <http://www.eff.org/effector/>.

Furthermore, EFF publishes a blog that highlights the latest news from around the Internet. DeepLinks (<http://www.eff.org/deeplinks/>) reports and analyzes newsworthy developments in technology. It also provides miniLinks, which direct readers to other news articles and commentary on these issues.

In addition to reporting hi-tech developments, EFF staff members have presented research and in-depth analysis on technology issues in no fewer than eighteen white

⁷ Guidestar Basic Report, Electronic Frontier Foundation, <http://www.guidestar.org/pqShowGsReport.do?npId=561625> (last visited July 10, 2007).

⁸ *Id.*

papers published since 2002. These papers, available at <http://www.eff.org/wp/>, provide information and commentary on such diverse issues as electronic voting, free speech, privacy and intellectual property.

EFF has also published several books to educate the public about technology and civil liberties issues. *Everybody's Guide to the Internet* (MIT Press 1994), first published electronically as *The Big Dummy's Guide to the Internet* in 1993, was translated into several languages, and is still sold by Powell's Books (<http://www.powells.com>). EFF also produced *Protecting Yourself Online: The Definitive Resource on Safety, Freedom & Privacy in Cyberspace* (HarperEdge 1998), a "comprehensive guide to self-protection in the electronic frontier," which can be purchased via Amazon.com (<http://www.amazon.com>). Finally, *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design* (O'Reilly 1998) revealed technical details on encryption security to the public. The book is available online at <http://cryptome.org/cracking-des.htm> and for sale at Amazon.com.

EFF also broadcasts podcasts of interviews with EFF staff and outside experts. *Line Noise* is a five-minute audio broadcast on EFF's current work, pending legislation, and technology-related issues. A listing of *Line Noise* podcasts is available at <feed://www.eff.org/rss/linenoisemp3.xml> and <feed://www.eff.org/rss/linenoiseogg.xml>.

Due to these extensive publication activities, EFF is a "representative of the news media" under the FOIA and agency regulations.

Request for a Public Interest Fee Waiver

EFF is entitled to a waiver of duplication fees because disclosure of the requested information is in the public interest within the meaning of 5 U.S.C. § 552(a)(4)(A)(iii) and 28 C.F.R. § 16.11(k). To determine whether a request meets this standard, Department of Justice components determine whether "[d]isclosure of the requested information is likely to contribute significantly to public understanding of the operations or activities of the government," and whether such disclosure "is not primarily in the commercial interest of the requester." 28 C.F.R. §§ 16.11(k)(i), (ii). This request clearly satisfies these criteria.

First, the DOJ's participation in a discussion to expand electronic communications surveillance capabilities concerns "the operations or activities of the government." 28 C.F.R. § 16.11(k)(2)(i).

Second, disclosure of the requested information will "contribute to an understanding of government operations or activities." 28 C.F.R. § 16.11(k)(2)(ii) (internal quotation marks omitted). EFF has requested information that will shed light on the nature of the DOJ's Internet surveillance technology and the reasons behind the DOJ's stated need for updated electronic communications surveillance capabilities.

Third, the requested material will "contribute to public understanding" of the DOJ's

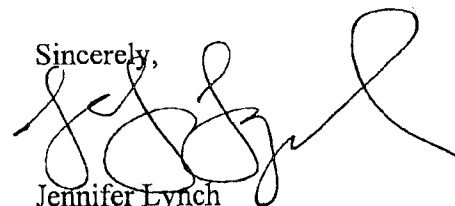
proposals to expand its surveillance capabilities and the need for that expansion. 28 C.F.R. § 16.11(k)(2)(iii) (internal quotation marks omitted). This information will contribute not only to EFF's understanding of the DOJ's surveillance activity, but to the understanding of a reasonably broad audience of persons interested in the subject. EFF will make the information it obtains under the FOIA available to the public and the media through its web site and newsletter, which highlight developments concerning privacy and civil liberties issues, and/or other channels discussed more fully above.

Fourth, the disclosure will "contribute significantly" to the public's knowledge and understanding of the DOJ's use of electronic surveillance. 28 C.F.R. § 16.11(k)(2)(iv) (internal quotation marks omitted). Disclosure of the requested information will help inform the public about the DOJ's need for expanded surveillance capabilities, as well as contribute to the public debate about whether and how proposed technological changes should be employed. The ability of law enforcement agencies to monitor new forms of electronic communications technology has important implications for the American public in the digital age. Law enforcement's ability to counter criminal threats and fulfill its duty to protect the American public, the consequent risk and potential for abuse due to such monitoring, and the possible economic and technological effect new regulations could have upon burgeoning technologies are all an important part of the public debate.

Furthermore, a fee waiver is appropriate here because EFF has no commercial interest in the disclosure of the requested records. 28 C.F.R. § 16.11(k)(3). EFF is a 501(c)(3) nonprofit organization, and will derive no commercial benefit from the information at issue here.

Thank you for your consideration of this request. If you have any questions or concerns, please do not hesitate to contact me at (415) 436-9333 x. 136. As the FOIA and applicable regulations provide, I will anticipate a determination on our request for expedited processing within 10 calendar days and a determination with respect to the disclosure of requested records within 20 working days.

Sincerely,



Jennifer Lynch
Staff Attorney

Attachments



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

October 21, 2009

Mr. David L. Sobel
Senior Counsel
Electronic Frontier Foundation
Suite 650
1875 Connecticut Avenue, Northwest
Washington, DC 20009

FOIPA No.: 1138791
Subject: USA PATRIOT Act /
Re-Authorization of Three
Provisions

Dear Mr. Sobel:

This is in reference to your request to the U.S. Department of Justice (DOJ), Federal Bureau of Investigation (FBI) Headquarters, for expedition of your Freedom of Information Act (FOIA) request dated September 25, 2009. Your FOIA request seeks information on the "Justice Department's recommendations on the three provisions of the Foreign Intelligence Surveillance Act (FISA) currently scheduled to expire on December 31, 2009", specifically the three provisions "Roving Wiretaps" (USA PATRIOT Act Section 206); "Business Records" (USA PATRIOT Act Section 215); and "Lone Wolf" (Intelligence Reform and Terrorism Prevention Act of 2004 Section 6001). You requested expedited processing pursuant to the Department of Justice standard permitting expedition for requests involving "[a]n urgency to inform the public about an actual or alleged federal government activity, if made by a person primarily engaged in disseminating information." 28 C.F.R. §16.5 (d)(1)(ii). Your request for expedition has been approved.

By separate letter dated October 21, 2009, the FBI acknowledged your FOIA request and advised that you that your FOIA request has been assigned FOIPA Request No. 1138791, and we have begun to conduct a search for potentially responsive records. Once the FBI completes its search for all records potentially responsive to your FOIA request, you will be advised as to the outcome of this search effort.

With respect to the portion of your letter seeking a waiver of the customary fees, we will make a decision once our records search is completed. In the event that your request for a fee waiver is denied, you will be notified of any applicable fees prior to the processing of any responsive records.

Sincerely yours,

David M. Hardy
Section Chief
Record/Information
Dissemination Section
Records Management Division

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC FRONTIER)	
FOUNDATION)	
)	
Plaintiff,)	
)	
v.)	Civil Action No. 06-1988 (ESH)
)	
DEPARTMENT OF HOMELAND)	
SECURITY,)	
)	
Defendant.)	
)	

STIPULATED DISMISSAL OF PLAINTIFF'S SECOND CAUSE OF ACTION

Plaintiff Electronic Frontier Foundation (EFF) and Defendant Department of Homeland Security (DHS), by counsel, hereby stipulate and agree as follows:

1. Defendant DHS has granted news media status to Plaintiff EFF based on the representations contained in EFF's FOIA requests, which demonstrate that EFF is an "entity that is organized and operated to publish or broadcast news to the public." 6 C.F.R. § 5.11(b)(6). Defendant DHS will continue to regard Plaintiff EFF as a "representative of the news media" absent a change in circumstances that indicates that EFF is no longer an "entity that is organized and operated to publish or broadcast news to the public." 6 C.F.R. § 5.11(b)(6).
2. Accordingly, the parties herewith agree to the dismissal of Plaintiff EFF's Second Cause of Action, related to EFF's status as a "representative of the news media."
3. The parties further agree that each will pay its own fees and costs for work on the dismissed claim.

SO STIPULATED AND AGREED this 27th day of February, 2007.

Case 1:06-cv-01988-ESH Document 15 Filed 02/27/2007 Page 2 of 2

/s/ David L. Sobel
DAVID L. SOBEL
D.C. Bar 360418

MARCIA HOFMANN
D.C. Bar 484136

ELECTRONIC FRONTIER FOUNDATION
1875 Connecticut Avenue, N.W.
Suite 650
Washington, D.C. 20009
(202) 797-9009

Counsel for Plaintiff

PETER D. KEISLER
Assistant Attorney General

JEFFREY A. TAYLOR
United States Attorney

ELIZABETH J. SHAPIRO
D.C. Bar 418925
Assistant Branch Director
U.S. Department of Justice
Civil Division, Federal Programs Branch

/s/ John R. Coleman
JOHN R. COLEMAN
Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW, Room 6118
Washington, D.C. 20530
(202) 514-4505

Counsel for Defendant



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 52276
6 February 2007

Ms. Marcia Hofmann
Electronic Frontier Foundation
1875 Connecticut Avenue, NW
Suite 650
Washington, DC 20009

Dear Ms. Hofmann:

This is an initial response to your Freedom of Information Act (FOIA) request submitted via facsimile on 23 January 2007, which was received by this office on 24 January 2007, for all agency records (including, but not limited to, electronic records) related to the NSA's review of and input on the configuration of the Microsoft Windows Vista operating system ("Vista"). Your request has been assigned Case Number 52276.

As we began to process your request, we realized that the first page of the actual request was missing from your 18-page facsimile package. On 1 February 2007, a member of my staff contacted you to advise you of this fact. As a result, you submitted another facsimile of your original five-page request, which we received and have begun to process. There is certain information relating to this processing about which the FOIA and applicable Department of Defense (DoD) and NSA/CSS regulations require we inform you.

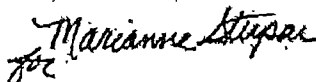
For purposes of this request and based on the information you provided in your letter, you are considered a representative of the media. Unless you qualify for a fee waiver or reduction, you must pay for duplication in excess of the first 100 pages. Your request for a fee waiver has been granted. In addition, please be advised your request for expedited treatment has been accepted. We are currently in the process of searching for responsive documents and will notify you of the status of your request as soon as that search has been completed.

Correspondence related to your request should include the case number assigned to your request, which is included in the first paragraph of this letter. Your letter should be addressed to National Security Agency, FOIA Office

FOIA Case: 52276

(DC34), 9800 Savage Road STE 6248, Ft. George G. Meade, MD 20755-6248
or may be sent by facsimile to 443-479-3612. If sent by fax, it should be
marked for the attention of the FOIA office. The telephone number of the FOIA
office is 301-688-6527.

Sincerely,

Handwritten signature of Marianne Stepan in cursive script.

PAMELA N. PHILLIPS
Chief
FOIA/PA Office

The New York Times® Reprints

This copy is for your personal, noncommercial use only. You can order presentation-ready copies for distribution to your colleagues, clients or customers [here](#) or use the "Reprints" tool that appears next to any article. Visit www.nytreprints.com for samples and additional information. [Order a reprint of this article now.](#)



September 27, 2010

U.S. Tries to Make It Easier to Wiretap the Internet

By **CHARLIE SAVAGE**

WASHINGTON — Federal law enforcement and national security officials are preparing to seek sweeping new regulations for the Internet, arguing that their ability to wiretap criminal and terrorism suspects is “going dark” as people increasingly communicate online instead of by telephone.

Essentially, officials want Congress to require all services that enable communications — including encrypted e-mail transmitters like BlackBerry, social networking Web sites like [Facebook](#) and software that allows direct “peer to peer” messaging like [Skype](#) — to be technically capable of complying if served with a wiretap order. The mandate would include being able to intercept and unscramble encrypted messages.

The bill, which the Obama administration plans to submit to lawmakers next year, raises fresh questions about how to balance security needs with protecting privacy and fostering innovation. And because security services around the world face the same problem, it could set an example that is copied globally.

James X. Dempsey, vice president of the Center for Democracy and Technology, an Internet policy group, said the proposal had “huge implications” and challenged “fundamental elements of the Internet revolution” — including its decentralized design.

“They are really asking for the authority to redesign services that take advantage of the unique, and now pervasive, architecture of the Internet,” he said. “They basically want to turn back the clock and make Internet services function the way that the telephone system used to function.”

But law enforcement officials contend that imposing such a mandate is reasonable and necessary to prevent the erosion of their investigative powers.

“We’re talking about lawfully authorized intercepts,” said [Valerie E. Caproni](#), general counsel for the [Federal Bureau of Investigation](#). “We’re not talking expanding authority. We’re talking about preserving our ability to execute our existing authority in order to protect the public safety and national security.”

Investigators have been concerned for years that changing communications technology could damage their ability to conduct surveillance. In recent months, officials from the F.B.I., the Justice Department, the [National Security Agency](#), the White House and other agencies have been meeting to develop a proposed solution.

There is not yet agreement on important elements, like how to word statutory language defining who counts as a communications service provider, according to several officials familiar with the deliberations.

But they want it to apply broadly, including to companies that operate from servers abroad, like Research in Motion, the Canadian maker of BlackBerry devices. In recent months, that company has [come into conflict](#) with the governments of Dubai and India over their inability to conduct surveillance of messages sent via its encrypted service.

In the United States, phone and broadband networks are already required to have interception capabilities, under a 1994 law called the [Communications Assistance to Law Enforcement Act](#). It aimed to ensure that government surveillance abilities would remain intact during the evolution from a copper-wire phone system to digital networks and cellphones.

Often, investigators can intercept communications at a switch operated by the network company. But sometimes — like when the target uses a service that encrypts messages between his computer and its servers — they must instead serve the order on a service provider to get unscrambled versions.

Like phone companies, communication service providers are subject to wiretap orders. But the 1994 law does not apply to them. While some maintain interception capacities, others wait until they are served with orders to try to develop them.

The F.B.I.'s operational technologies division spent \$9.75 million last year helping communication companies — including some subject to the 1994 law that had difficulties — do so. And its 2010 budget included \$9 million for a “Going Dark Program” to bolster its electronic surveillance capabilities.

Beyond such costs, Ms. Caproni said, F.B.I. efforts to help retrofit services have a major shortcoming: the process can delay their ability to wiretap a suspect for months.

Moreover, some services encrypt messages between users, so that even the provider cannot unscramble them.

There is no public data about how often court-approved surveillance is frustrated because of a service's technical design.

But as an example, one official said, an investigation into a drug cartel earlier this year was stymied because smugglers used peer-to-peer software, which is difficult to intercept because it is not routed through a central hub. Agents eventually installed surveillance equipment in a suspect's office, but that tactic was “risky,” the official said, and the delay “prevented the interception of pertinent communications.”

Moreover, according to several other officials, after the failed Times Square bombing in May, investigators discovered that the suspect, **Faisal Shahzad**, had been communicating with a service that lacked prebuilt interception capacity. If he had aroused suspicion beforehand, there would have been a delay before he could have been wiretapped.

To counter such problems, officials are coalescing around several of the proposal's likely requirements:

¶ Communications services that encrypt messages must have a way to unscramble them.

¶ Foreign-based providers that do business inside the United States must install a domestic office capable of performing intercepts.

¶ Developers of software that enables peer-to-peer communication must redesign their service to allow interception.

Providers that failed to comply would face fines or some other penalty. But the proposal is likely to direct companies to come up with their own way to meet the mandates. Writing any statute in “technologically neutral” terms would also help prevent it from becoming obsolete, officials said.

Even with such a law, some gaps could remain. It is not clear how it could compel compliance by overseas services that do no domestic business, or from a “freeware” application developed by volunteers.

In their battle with Research in Motion, countries like Dubai have sought leverage by threatening to block BlackBerry data from their networks. But Ms. Caproni said the F.B.I. did not support filtering the Internet in the United States.

Still, even a proposal that consists only of a legal mandate is likely to be controversial, said [Michael A. Sussmann](#), a former Justice Department lawyer who advises communications providers.

“It would be an enormous change for newly covered companies,” he said. “Implementation would be a huge technology and security headache, and the investigative burden and costs will shift to providers.”

Several privacy and technology advocates argued that requiring interception capabilities would create holes that would inevitably be exploited by hackers.

[Steven M. Bellovin](#), a [Columbia University](#) computer science professor, pointed to an [episode in Greece](#): In 2005, it was discovered that hackers had taken advantage of a legally mandated wiretap function to spy on top officials’ phones, including the prime minister’s.

“I think it’s a disaster waiting to happen,” he said. “If they start building in all these back doors, they will be exploited.”

[Susan Landau](#), a Radcliffe Institute of Advanced Study fellow and former Sun Microsystems engineer, argued that the proposal would raise costly impediments to innovation by small startups.

“Every engineer who is developing the wiretap system is an engineer who is not building in

greater security, more features, or getting the product out faster,” she said.

Moreover, providers of services featuring user-to-user encryption are likely to object to watering it down. Similarly, in the late 1990s, encryption makers fought off a proposal to require them to include a back door enabling wiretapping, arguing it would cripple their products in the global market.

But law enforcement officials rejected such arguments. They said including an interception capability from the start was less likely to inadvertently create security holes than retrofitting it after receiving a wiretap order.

They also noted that critics predicted that the 1994 law would impede cellphone innovation, but that technology continued to improve. And their envisioned decryption mandate is modest, they contended, because service providers — not the government — would hold the key.

“No one should be promising their customers that they will thumb their nose at a U.S. court order,” Ms. Caproni said. “They can promise strong encryption. They just need to figure out how they can provide us plain text.”



U.S. Department of Justice

Criminal Division

Office of Enforcement Operations

Washington, D.C. 20530

CRM-201000724F

Jennifer Lynch
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

OCT - 4 2010

Dear Ms. Lynch:

The U.S. Department of Justice (DOJ), Criminal Division acknowledges receipt of your Freedom of Information Act (FOIA) request dated September 28, 2010. In that request, you asked for copies of:

all agency records created on or after January 1, 2006 (including, but not limited to, electronic records) discussing, concerning, or reflecting:

1. any problems, obstacles or limitations that hamper the DOJ's current ability to conduct surveillance on communications systems or networks including, but not limited to, encrypted services like Blackberry (RIM), social networking sites like Facebook, peer-to-peer messaging services like Skype, etc.;
2. any communications or discussions with the operators of communications systems or networks (including, but not limited to, those providing encrypted communications, social networking, and peer-to-peer messaging services), or with equipment manufacturers and vendors, concerning technical difficulties the DOJ has encountered in conducting authorized electronic surveillance;
3. any communications or discussions concerning technical difficulties the DOJ has encountered in obtaining assistance from non-U.S.-based operators of communications systems or networks, or with equipment manufacturers and vendors in the conduct of authorized electronic surveillance;
4. any communications or discussions with the operators of communications systems or networks, or with equipment manufacturers and vendors, concerning development and needs related to electronic communications surveillance-enabling technology;
5. any communications or discussions with foreign government representatives or trade groups about trade restrictions or import or export controls related to electronic communications surveillance-enabling technology;

FILE COPY

KUE 10/4/10

6. any briefings, discussions, or other exchanges between DOJ officials and members of the Senate or House of Representatives concerning implementing a requirement for electronic communications surveillance-enabling technology, including, but not limited to, proposed amendments to the Communications Assistance to Law Enforcement Act (CALEA).

Your request has been assigned file number 201000724F. Please refer to this number in any future correspondence with this Unit.

We will conduct a search to locate any records that the Criminal Division has that are within the scope of your request. Once we have completed our search, we will notify you as to our disposition of your request.

In addition to your request for records, you asked that we expedite the processing of your request. Requests will be given expedited treatment whenever it is determined that they involve:

1. Circumstances in which the lack of expedited treatment could reasonably be expected to pose an imminent threat to the life or physical safety of an individual;
2. An urgency to inform the public about an actual or alleged federal government activity, if made by a person primarily engaged in disseminating information;
3. The loss of substantial due process rights; or
4. A matter of widespread and exceptional media interest in which there exists possible questions about the government's integrity which affect public confidence.

28 C.F.R. § 16.5(d).

Requests for expedited treatment must be accompanied by a statement, certified to be true and correct to the best of the requester's knowledge and belief, that explains in detail the basis for requesting expedited processing. 28 C.F.R. § 16.5(d)(3). You requested expedited processing based on news reports that next year, the Obama administration is planning to propose new legislation requiring all services that enable communications to be technically capable of complying if served with a wiretap order.

After careful review, your request for expedited processing has been denied. Specifically, we do not believe that your request for information about legislation that may or may not be proposed to Congress next year satisfies the criteria for expedited processing.

You may appeal the denial of your request for expedited processing by writing to:

Office of Information Policy
United States Department of Justice
1425 New York Ave., N.W., Suite 11050
Washington, D.C. 20530-0001

Both the envelope and appeal letter should be clearly marked "FOIA/PA Appeal." Department regulations provide that such appeals must be received by the Office of Information Policy within sixty days of the date of this letter. 28 C.F.R. § 16.9. If you exercise this right and your appeal is denied, you also have the right to seek judicial review of this action in the federal judicial district (1) in which you reside, (2) in which you have your principal place of business, (3) in which the records denied are located, or (4) for the District of Columbia. If you elect to file an appeal, please include the Criminal Division file number above in your letter to the Office of Information Policy.

Finally, you requested a fee waiver. We will consider your fee waiver request once we determine what records we maintain within the scope of your records request (if any) and whether any fees will be incurred in the processing of your records request.

If you have any questions regarding your request, please contact us at 202-616-0307. Thank you for your interest in the Criminal Division.

Sincerely,

Rena Y. Kim, Chief
Freedom of Information/Privacy Act Unit