

1 Jennifer Lynch (SBN 240701)  
jlynch@eff.org  
2 ELECTRONIC FRONTIER FOUNDATION  
454 Shotwell Street  
3 San Francisco, CA 94110  
Telephone: (415) 436-9333  
4 Facsimile: (415) 436-9993

5 David L. Sobel (*pro hac vice pending*)  
sobel@eff.org  
6 ELECTRONIC FRONTIER FOUNDATION  
1818 N Street, N.W.  
7 Suite 410  
Washington, DC 20036  
8 Telephone: (202) 797-9009 x104  
Facsimile: (202) 707-9066

9 Attorneys for Plaintiff  
10 ELECTRONIC FRONTIER FOUNDATION

11 **UNITED STATES DISTRICT COURT**  
12 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**  
13 **SAN FRANCISCO DIVISION**

14 ELECTRONIC FRONTIER FOUNDATION, )  
15 )  
16 Plaintiff, ) **COMPLAINT FOR INJUNCTIVE**  
17 v. ) **RELIEF FOR VIOLATION OF THE**  
18 DEPARTMENT OF JUSTICE, ) **FREEDOM OF INFORMATION ACT,**  
19 Defendant. ) **5 U.S.C. § 552**  
20 \_\_\_\_\_ )

21 1. This is an action under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, for  
22 injunctive and other appropriate relief. Plaintiff seeks the expedited processing and release of  
23 records that Plaintiff requested from Defendant Department of Justice and its components, Federal  
24 Bureau of Investigation, Drug Enforcement Agency, and Criminal Division, concerning the  
25 agency’s efforts to push for changes to federal surveillance law to ensure that all services that  
26 enable communications be technically capable of complying with a wiretap order. The requested  
27 records concern a matter about which there is “[a]n urgency to inform the public about an actual or  
28 alleged federal government activity,” and were “made by a person primarily engaged in

1 disseminating information.” 5 U.S.C. § 552(a)(6)(E)(v)(II); 28 C.F.R. § 16.5(d)(1)(ii). Therefore,  
2 Plaintiff is statutorily entitled to the expedited treatment it seeks.

3 **PARTIES**

4 2. Plaintiff Electronic Frontier Foundation (EFF) is a not-for-profit corporation  
5 established under the laws of the Commonwealth of Massachusetts, with offices in San Francisco,  
6 California and Washington, DC. EFF is a donor-supported membership organization that works to  
7 inform policymakers and the general public about civil liberties issues related to technology and to  
8 act as a defender of those liberties. In support of its mission, EFF uses the FOIA to obtain and  
9 disseminate information concerning the activities of federal agencies.

10 3. Defendant Department of Justice (DOJ) is a Department of the Executive Branch of  
11 the United States Government. DOJ is an “agency” within the meaning of 5 U.S.C. § 552(f). The  
12 Federal Bureau of Investigation (FBI), Drug Enforcement Agency (DEA), and Criminal Division  
13 are components of Defendant DOJ.

14 **JURISDICTION**

15 4. This Court has both subject matter jurisdiction over this action and personal  
16 jurisdiction over the parties pursuant to 5 U.S.C. §§ 552(a)(4)(B) and 552(a)(6)(C)(i). This Court  
17 also has jurisdiction over this action pursuant to 28 U.S.C. § 1331.

18 **VENUE AND INTRADISTRICT ASSIGNMENT**

19 5. Venue is proper in this district under 5 U.S.C. § 552(a)(4)(B) and 28 U.S.C. §  
20 1391(e).

21 6. Assignment to the San Francisco division is proper pursuant to Local Rule 3-2(c)  
22 and (d) because a substantial portion of the events giving rise to this action occurred in this district  
23 and division, where Plaintiff is headquartered.

24 //

25 //

26 //

27 //

28 //

1 **FACTUAL ALLEGATIONS**

2 **Federal Law Enforcement and Intelligence Agencies Prepare to Seek Legislation Requiring**  
3 **All Communications Providers Build in a Back Door to Allow Government Spying**

4 7. On September 27, 2010, the *New York Times* reported:

5 Federal law enforcement and national security officials are preparing  
6 to seek sweeping new regulations for the Internet[.] . . .

7 Essentially, officials want Congress to require all services that enable  
8 communications — including encrypted e-mail transmitters like  
9 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.

10 Charlie Savage, *U.S. Tries to Make it Easier to Wiretap the Internet*, N.Y. Times at A1 (Sept. 27,  
11 2010). The *Times* further reported that officials from the FBI, the Justice Department, the National  
12 Security Agency as well as other agencies had been meeting with White House officials in the last  
13 few months to develop a proposal and that the Obama administration planned to submit legislation  
14 to Congress next year. *Id.*

15 8. Immediately after the *Times* reported on the agencies’ plans, many other national  
16 and international news organizations also reported on the story. *See, e.g.*, Glenn Greenwald, *The*  
17 *Obama Administration’s War on Privacy*, Salon.com (Sept. 27, 2010);<sup>1</sup> Kit Eaton, *What a*  
18 *Wiretappable Internet Could Mean for Facebook, Apple, Google, and You*, Fast Company (Sept.  
19 27, 2010);<sup>2</sup> Lolita C. Baldor, *Report: US Would Make Internet Wiretaps Easier*, Washington Post  
20 (Sept. 27, 2010);<sup>3</sup> Ellen Nakashima, *Administration Seeks Ways to Monitor Internet*  
21 *Communications*, Washington Post (Sept. 27, 2010);<sup>4</sup> PBS News Hour, *Proposal Could Expand*  
22 *Government’s Web Wiretapping Efforts* (Sept. 27, 2010);<sup>5</sup> Declan McCullagh, *US Government to*  
23 *Seek Intercept Powers on Internet*, CNET News (Sept. 27, 2010);<sup>6</sup> Ryan Singel, *FBI Drive for*

24 \_\_\_\_\_  
25 <sup>1</sup> [http://www.salon.com/news/opinion/glenn\\_greenwald/2010/09/27/privacy/index.html](http://www.salon.com/news/opinion/glenn_greenwald/2010/09/27/privacy/index.html).

26 <sup>2</sup> <http://www.fastcompany.com/1691505/wiretap-emails-facebook-apple-google>.

27 <sup>3</sup> <http://www.washingtonpost.com/wp-dyn/content/article/2010/09/27/AR2010092700719.html>.

28 <sup>4</sup> <http://www.washingtonpost.com/wp-dyn/content/article/2010/09/27/AR2010092703244.html>.

<sup>5</sup> [http://www.pbs.org/newshour/bb/government\\_programs/july-dec10/wiretap\\_09-27.html](http://www.pbs.org/newshour/bb/government_programs/july-dec10/wiretap_09-27.html).

<sup>6</sup> <http://www.zdnet.co.uk/news/regulation/2010/09/27/us-government-to-seek-intercept-powers-on-internet-40090294/>.

1 *Encryption Backdoors Is Déjà Vu for Security Experts*, *Wired* (Sept. 27, 2010),<sup>7</sup> Dan Goodin, *Feds*  
2 *Want Backdoors Built into VoIP and Email*, *The Register* (Sept. 27, 2010).<sup>8</sup>

3 9. Shortly after the *Times* article appeared, FBI Director Robert Mueller publicly  
4 called for changes to federal law to allow FBI agents greater ability to intercept communications.  
5 See Robert S. Mueller, Director, Federal Bureau of Investigation, *Speech to Preparedness Group*  
6 *Conference*, Washington, D.C. (Oct. 6, 2010) available at: [http://www.fbi.gov/news/speeches](http://www.fbi.gov/news/speeches/countering-the-terrorism-threat)  
7 [/countering-the-terrorism-threat](http://www.fbi.gov/news/speeches/countering-the-terrorism-threat). He stated,

8 One lesson we have learned in recent years is the need to ensure that the  
9 laws by which we operate keep pace with new threats and new  
10 technology. . . .

11 In some instances, communications providers are not able to provide the  
12 electronic communications we seek in response to a court order. Many  
13 providers are not currently required to build or maintain intercept  
14 capabilities in their operating systems. As a result, they are often not  
15 equipped to provide timely assistance.

16 Critical laws covering this area have not been updated since 1994[.] . . .

17 We want to ensure that our ability to intercept communications is not  
18 eroded by advances in technology—technology we all rely on to  
19 communicate.

20 *Id.*

21 10. On October 18, 2010, the *New York Times* published a second article on agency  
22 efforts to expand communications surveillance laws. See Charlie Savage, *Officials Push to Bolster*  
23 *Law on Wiretapping*, *N.Y. Times* at A1 (Oct. 18, 2010). The *Times* reported,

24 An Obama administration task force that includes officials from the  
25 Justice and Commerce Departments, the F.B.I. and other agencies  
26 recently began working on draft legislation to strengthen and expand  
27 the Communications Assistance to Law Enforcement Act[.]

28 *Id.* The article further noted, “The Obama administration is circulating several ideas for  
legislation,” and reiterated that, although “[t]here is not yet agreement over the details . . . the  
administration intends to submit a package to Congress next year.” *Id.*

11. The FBI has invested tens of millions of dollars in technology and resources to

<sup>7</sup> <http://www.wired.com/threatlevel/2010/09/fbi-backdoors/>.

<sup>8</sup> [http://www.theregister.co.uk/2010/09/27/encryption\\_backdoor\\_legislation/](http://www.theregister.co.uk/2010/09/27/encryption_backdoor_legislation/).

1 enable it to intercept communications. The September 27th *Times* article noted the “F.B.I.’s  
2 operational technologies division spent \$9.75 million last year helping communication companies  
3 — including some subject to the 1994 law that had difficulties — [develop interception capacities].  
4 And its 2010 budget included \$9 million for a ‘Going Dark Program’ to bolster its electronic  
5 surveillance capabilities.” Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*. The  
6 October 18th *Times* article noted the FBI spends “about \$20 million a year” to help companies  
7 comply with wiretap orders. Savage, *Officials Push to Bolster Law on Wiretapping*. The FBI’s  
8 2010 budget also included “\$20.5 million to ensure the FBI’s capability to develop wireless  
9 tracking and intercept technologies for 3rd Generation (3G) wireless networks are up to date.” See  
10 Federal Bureau of Investigation Budget and Performance Summary *available at*:  
11 <http://www.justice.gov/jmd/2010summary/pdf/fbi-bud-summary.pdf>.

12 12. Other than two examples provided by the FBI in Director Mueller’s speech, *see*  
13 Mueller, *Speech to Preparedness Group Conference* (noting FBI’s difficulties intercepting  
14 communications in a drug cartel case and a child exploitation case), there is no official information  
15 on how necessary this proposed technological and legislative change is for government  
16 surveillance. The September 27th *Times* article noted, “There is no public data about how often  
17 court-approved surveillance is frustrated because of a service’s technical design.” Savage, *U.S.*  
18 *Tries to Make It Easier to Wiretap the Internet*. Further, in the examples mentioned by Director  
19 Mueller, the FBI was not prevented from obtaining the information it sought but was able to get it  
20 using other investigative techniques. Mueller, *Speech to Preparedness Group Conference*.

### 21 **Plaintiff’s FOIA Requests and Requests for Expedited Processing**

22 13. In a letter dated May 21, 2009 and sent by facsimile to the FBI, Plaintiff requested  
23 under the FOIA all agency records, including electronic records, from 2007 to the present  
24 concerning the Going Dark Program, including but not limited to a) all records that describe the  
25 Going Dark Program; b) all Privacy Impact Assessments prepared for the Going Dark Program;  
26 and c) all System of Records Notices (“SORNs”) that discuss or describe the Going Dark Program.

27 14. The FBI acknowledged Plaintiff’s request via a letter dated May 26, 2009. By letter  
28 dated August 21, 2009, the FBI stated it had begun the search. By letters dated January 7, 2010,

1 July 8, 2010 and October 6, 2010, the FBI stated it had assigned an analyst to review Plaintiff's  
2 request.

3 15. To date, the FBI has not produced any documents in response to Plaintiff's request  
4 described in paragraph 13 nor informed Plaintiff of an anticipated date for the completion of the  
5 processing of the requests.

6 16. In letters dated September 28, 2010 and sent by facsimile to the FBI, DEA, and DOJ  
7 Criminal Division, Plaintiff requested under the FOIA all records created on or after January 1,  
8 2006 (including, but not limited to, electronic records) discussing, concerning, or reflecting:

9 a) any problems, obstacles or limitations that hamper the agency's  
10 current ability to conduct surveillance on communications systems or  
11 networks including, but not limited to, encrypted services like  
Blackberry (RIM), social networking sites like Facebook, peer-to-  
peer messaging services like Skype, etc.;

12 b) any communications or discussions with the operators of  
13 communications systems or networks (including, but not limited to,  
14 those providing encrypted communications, social networking, and  
15 peer-to-peer messaging services), or with equipment manufacturers  
and vendors, concerning technical difficulties the agency has  
encountered in conducting authorized electronic surveillance;

16 c) any communications or discussions concerning technical  
17 difficulties the agency has encountered in obtaining assistance from  
18 non-U.S.-based operators of communications systems or networks, or  
with equipment manufacturers and vendors in the conduct of  
authorized electronic surveillance;

19 d) any communications or discussions with the operators of  
20 communications systems or networks, or with equipment  
21 manufacturers and vendors, concerning development and needs  
22 related to electronic communications surveillance-enabling  
23 technology;

24 e) any communications or discussions with foreign government  
25 representatives or trade groups about trade restrictions or import or  
26 export controls related to electronic communications surveillance-  
enabling technology;

27 f) any briefings, discussions, or other exchanges between agency  
28 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)

17. In its September 28 letters, Plaintiff also formally requested that the processing of

1 these requests be expedited because they pertain to information about which there is “[a]n urgency  
2 to inform the public about an actual or alleged federal government activity,” and were “made by a  
3 person primarily engaged in disseminating information.” 5 U.S.C. § 552(a)(6)(E)(v)(II); 28 C.F.R.  
4 § 16.5(d)(1)(ii).

5 18. On information and belief, the FBI, DEA, and DOJ Criminal Division received  
6 Plaintiff’s request letters, described in paragraphs 16 & 17, on September 28, 2010.

7 19. By letter dated October 1, 2010, DEA acknowledged receipt of Plaintiff’s FOIA  
8 request.

9 20. By letter dated October 4, 2010, Defendant DOJ’s Criminal Division acknowledged  
10 receipt of Plaintiff’s FOIA request and informed Plaintiff that its request for expedited processing  
11 had been denied.

12 21. By letter dated October 20, 2010, the FBI acknowledged receipt of Plaintiff’s FOIA  
13 request and informed Plaintiff that its requests for a fee waiver and for expedited processing had  
14 been granted.

15 22. Not only has Defendant failed to expedite the processing of Plaintiff’s requests  
16 (notwithstanding the FBI’s purported grant of Plaintiff’s expedition request), but it has also  
17 exceeded the generally applicable twenty-day deadline for the processing of *any* FOIA request.

18 23. Plaintiff has exhausted the applicable administrative remedies with respect to all of  
19 its FOIA requests referenced herein.

20 24. Defendant has wrongfully withheld the requested records from Plaintiff.

21 **CAUSES OF ACTION**

22 **Violation of the Freedom of Information Act for Failure to Expedite Processing**

23 25. Plaintiff repeats and realleges paragraphs 1-24.

24 26. Defendant has violated the FOIA by failing to expedite the processing of Plaintiff’s  
25 FOIA requests.

26 27. Plaintiff has exhausted the applicable administrative remedies with respect to  
27 Defendant’s failure to expedite the processing of Plaintiff’s requests.

28 28. Plaintiff is entitled to injunctive relief with respect to the expedited processing of

1 the requested agency records.

2 **Violation of the Freedom of Information Act for Wrongful Withholding of Agency Records**

3 29. Plaintiff repeats and realleges paragraphs 1-24.

4 30. Defendant has wrongfully withheld agency records requested by Plaintiff by failing  
5 to comply with the statutory time limit for the processing of FOIA requests.

6 31. Plaintiff has exhausted the applicable administrative remedies with respect to  
7 Defendant's wrongful withholding of the requested records.

8 32. Plaintiff is entitled to injunctive relief with respect to the release and disclosure of  
9 the requested documents.

10 **REQUESTED RELIEF**

11 WHEREFORE, Plaintiff prays that this Court:

12 1. order Defendant and its components to process immediately the requested records in  
13 their entirety;

14 2. order Defendant and its components, upon completion of such expedited processing,  
15 to disclose the requested records in their entirety and make copies available to Plaintiff;

16 3. provide for expeditious proceedings in this action;

17 4. award Plaintiff its costs and reasonable attorneys fees incurred in this action; and

18 5. grant such other relief as the Court may deem just and proper.

19  
20 DATED: October 28, 2010

21 By \_\_\_\_\_

22 Jennifer Lynch, Esq.  
23 ELECTRONIC FRONTIER FOUNDATION  
454 Shotwell Street  
San Francisco, CA 94110

24 David L. Sobel (*pro hac vice pending*)  
25 ELECTRONIC FRONTIER FOUNDATION  
1818 N Street, N.W., Suite 410  
26 Washington, DC 20009

27 Attorneys for Plaintiff  
28 ELECTRONIC FRONTIER FOUNDATION



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28