

epic.org

June 6, 2013

VIA FACSIMILE 202-514-0563

Elizabeth Farris
 Supervisory Paralegal
 Office of Legal Counsel
 Room 5515, 950 Pennsylvania Avenue, NW
 Department of Justice
 Washington, DC 20530-0001
 (202) 514-2038

1718 Connecticut Ave NW
 Suite 200
 Washington DC 20009
 USA
 +1 202 483 1140 [tel]
 +1 202 483 1248 [fax]
 www.epic.org

Re: EPIC FOIA Request and Request for Expedited Processing – PRISM

Dear Ms. Farris:

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted on behalf of the Electronic Privacy Information Center ("EPIC"). As detailed below, EPIC seeks Office of Legal Counsel ("OLC") memorandums and opinions concerning the legal authority for the Federal Bureau of Investigation ("FBI") and National Security Agency's ("NSA") PRISM program.

Background

The PRISM program

On June 6, 2013, the Washington Post reported that the NSA and the FBI "are tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio, video, photographs, e-mails, documents and connection logs that enable analysts to track a person's movements and contacts over time."¹

This program, called PRISM, has reportedly been in operation since 2007. It allows direct access by the FBI and NSA, in real-time, to data held by Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple.² According to news reports, PRISM data accounts for nearly one in seven intelligence reports and was cited in 1,477 articles in the President's Daily Brief.³ The program "routinely collects a great deal of American [citizens'] content."⁴ According to news reports, in 2008 Congress gave the Justice Department the authority to seek orders from

¹ Barton Gellman and Laura Poitras, *U.S. intelligence mining data from nine U.S. Internet companies in broad secret program*, Wash. Post, June 6, 2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

² *Id.*

³ *Id.*

⁴ *Id.*

the Foreign Intelligence Surveillance Court ("FISC") to compel private companies to comply with the PRISM program.⁵ PRISM is run by the Special Source Operations division of the NSA.⁶

The Guardian newspaper reports that "[t]he program facilitates extensive, in-depth surveillance on both live communications and stored information. . . . It also opens the possibility of communications made entirely within the US being collected without warrants."⁷

The Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. §§ 1801 *et. seq.*, authorizes electronic surveillance of "foreign intelligence information" between "foreign powers" and "agents of foreign powers." The purpose of the FISA is to allow the Intelligence Community to participate *foreign* intelligence gathering, not domestic.⁸ The purpose of the FISC is to ensure that FISA investigations remain focused on foreign agents, not U.S. persons. As the Supreme Court explained just a few months ago, "Congress enacted the Foreign Intelligence Surveillance Act (FISA) to authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes. . . . In FISA, Congress authorized judges of the Foreign Intelligence Surveillance Court (FISC) to approve electronic surveillance for foreign intelligence purposes. . . ."⁹

For the PRISM program to be lawful, it would have to meet the legal requirements of both the FISA and, more generally, the Fourth Amendment of the Constitution.¹⁰ The Fourth Amendment protects against government searches both when the party being searched has a "reasonable expectation of privacy"¹¹ and also "[w]hen 'the Government obtains information by physically intruding' on persons, houses, papers, or effects."¹²

OLC Memorandums and Opinion

The Office of Legal Counsel definitively interprets the law for the Executive Branch; its legal opinions are binding on all federal agencies.¹³ "The Office drafts legal opinions of the

⁵ *Id.*

⁶ *Id.*

⁷ Glenn Greenwald and Ewen MacAskill, "NSA Taps in to Internet Giants' Systems to Mine User Data, Secret Files Reveals, The Guardian, June 6, 2013, <http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data>.

⁸ "This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused." S. Rep. No. 95-604(I) at 7 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908.

⁹ *Clapper v. Amnesty Int'l USA*, ___ U.S. ___, 133 S.Ct. 1138, 1143 (2013).

¹⁰ "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

¹¹ *Katz v. United States*, 389 U.S. 347 (1967).

¹² *Florida v. Jardines*, 569 U.S. ___, slip op. at *3 (2013).

¹³ See Brief of *Amicus Curiae* EPIC in Support of Appellants, *New York Times Co. v. U.S. Dep't of Justice*, No. 13-0422 (2d. Cir. filed April 22, 2013), available at <https://epic.org/amicus/foia/new-york-times/EPIC-et-al-Amici-Brief.pdf>.

Attorney General and also provides its own written opinions and oral advice" in response to Executive Branch requests.¹⁴

It would be the OLC's responsibility to draft legal memorandums and opinions interpreting the legality of the PRISM program under the Fourth Amendment, FISA, and other statutes. To the extent that the FBI and NSA may access the electronic communications, including content information, of U.S. persons using U.S. internet service providers, it would be the responsibility of the OLC to interpret the legality of those actions.

Requested Documents

1. All final legal analyses, memoranda, and opinions regarding the PRISM program, including, but not limited to, records addressing the Foreign Intelligence Surveillance Act, 50 U.S.C. §§1801 *et. seq.*, and the Fourth Amendment to the U.S. Constitution.

Request for Expedited Processing

This request warrants expedited processing because it is made by "a person primarily engaged in disseminating information..." and because it pertains to a matter about which there is an "urgency to inform the public about an actual or alleged federal government activity." 5 U.S.C. § 552(a)(6)(E)(v)(II) (2008); *Al-Fayed v. Cent. Intelligence Agency*, 254 F.3d 300, 306 (D.C. Cir. 2001).

EPIC is "primarily engaged in disseminating information." *Am. Civil Liberties Union v. Dep't of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

There is a particular urgency for the public to obtain information about the legal authority of law enforcement to obtain electronic communications about any U.S. person using Internet and online service providers. Only just recently has the public discovered that the NSA has also been collecting telephone data on potentially millions of U.S. persons.¹⁵ The revelation that the agency, through PRISM, may also be able to monitor user generated content, in real time, raises profound concerns about the ability of Americans to maintain any privacy from their government. "The participation of the internet companies in PRISM will add to the debate, ignited by the Verizon revelation, about the scale of surveillance by the intelligence services. Unlike the collection of those call records, this surveillance can include the content of communications and not just the metadata."¹⁶ Given the urgency of the situation, it is vital that the public understand the FBI and NSA's legal authority to obtain these records.

¹⁴ U.S. Dep't of Justice, Off. of Legal Counsel, <http://www.justice.gov/olc/> (March 2013).

¹⁵ Charlie Savage and Edward Wyatt, *U.S. Secretly Collecting Records of Verizon Calls*, N.Y. Times, June 5, 2013, <http://www.nytimes.com/2013/06/06/us/us-secretly-collecting-logs-of-business-calls.html>.

¹⁶ Glenn Greenwald and Ewen MacAskill, "NSA Taps in to Internet Giants' Systems to Mine User Data, Secret Files Reveals", The Guardian, June 6, 2013, <http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data>.

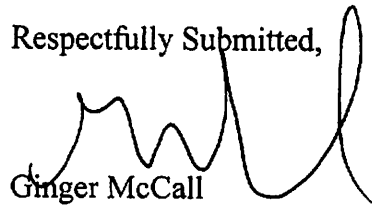
Request for "News Media" Fee Status

EPIC is a "representative of the news media" for fee waiver purposes. *EPIC v. Dep't of Defense*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on our status as a "news media" requester, we are entitled to receive the requested record with only duplication fees assessed. Further, because disclosure of this information will "contribute significantly to public understanding of the operations or activities of the government," any duplication fees should be waived.


Conclusion

Thank you for your consideration of this request. As 5 U.S.C. § 552(a)(6)(E)(ii)(I) provides, I will anticipate your determination on our request within ten (10) calendar days. I can be contacted at 202-483-1140 x 123 or foia@epic.org.

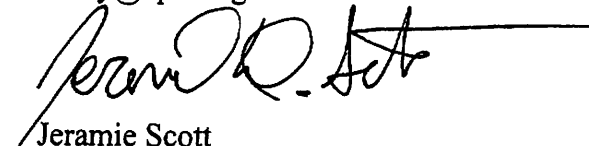
Respectfully Submitted,



Ginger McCall
Director, EPIC Open Government Program
mccall@epic.org



David Brody
EPIC Appellate Advocacy Fellow
brody@epic.org



Jeramie Scott
EPIC National Security Fellow
jscott@epic.org