



February 5, 2014

David M. Hardy, Chief
Record/Information Dissemination Section
Records Management Division
Federal Bureau of Investigation
Department of Justice
170 Marcel Drive
Winchester, VA 22602-4843
Email: foiparequest@ic.fbi.gov

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
WWW.ACLU.ORG

Via Email and UPS

Re: Request Under Freedom of Information Act

Dear Mr. Hardy:

This letter is a request by the American Civil Liberties Union Foundation (“ACLU”) under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552 *et seq.*, and the Department of Justice implementing regulations, 28 C.F.R. § 16.1 *et seq.* This request seeks records regarding the FBI’s use of processes, devices, hardware, software, or firmware known as “port readers.”

I. Background

In recent months, news reports have indicated that FBI officials were “sparring” with telecommunications and Internet service providers as the officials pushed for installation of port readers on providers’ networks.¹ As explained in *Foreign Policy*, port readers “make[] copies of emails as they flow through a network. Then, in practically an instant, the port reader dissects them, removing only the metadata that has been approved by a court.”

¹ Declan McCullagh, *FBI Pressures Internet Providers to Install Surveillance Software*, CNET (Aug. 2, 2013), <http://cnet.co/1eGnxO4>; see also Shane Harris, *Meet the Spies Doing the NSA’s Dirty Work*, *Foreign Policy*, Nov. 22, 2013, <http://atfp.co/1j5EwwN>.

The specific metadata collected includes “as many as 13 individual fields of information.”² Reportedly, these fields contain not only “traditional metadata” such as the sender and recipient of a message, but also the route a message takes over a network, port numbers, and IP addresses, which can reveal a computer’s location and its user.³

The *Foreign Policy* article further explained that port readers were developed at least partially by the FBI’s Data Intercept Technology Unit (DITU), which works closely with large U.S. telecommunications companies including AT&T, Verizon, and Sprint, as well as Internet service providers. DITU also works with the National Security Agency (NSA), collecting data for its PRISM program.⁴

According to the same article, the FBI wishes to install port readers on providers’ networks “so that the government can collect large volumes of data about emails and Internet traffic.” Although it remains unclear how many companies are cooperating with port reader installation, “at least two firms are pushing back” against installing it, largely because it initially captures entire emails without a warrant.⁵

Traditional metadata, especially when collected in large volumes, is extremely sensitive. Knowing who a person exchanges emails with, when, and how often can reveal when relationships end or new ones begin, when friendships grow closer or drift apart, and when professional conflicts arise or alliances are formed. Even the metadata of a single message, when sent from a journalistic source, for instance, or to an attorney or therapist, can potentially be very sensitive. The possible addition of location data only increases the sensitivity of the information.

As Judge Leon of the District Court for the District of Columbia explained when ruling that the NSA’s bulk collection of telephone metadata was likely unconstitutional, metadata can “reveal an entire mosaic—a vibrant and constantly updating picture of the person’s life.” *Klayman v. Obama*, Civil Action No. 13-0851 (RJL), 2013 WL 6571596, at *21 (D.D.C. Dec. 16, 2013). Americans have a significant interest in the privacy of their communications, including the metadata associated with their communications. Accordingly, this request seeks records related to the government’s use of port readers to collect Internet metadata and other data.

² Shane Harris, *Meet the Spies Doing the NSA’s Dirty Work*, *Foreign Policy*, Nov. 22, 2013, <http://atfp.co/lj5EwwN>.

³ *Id.*

⁴ *Id.*

⁵ *Id.*

II. Requested Records

The ACLU seeks records regarding the port reader processes, devices, hardware, software, or firmware discussed in the CNET and *Foreign Policy* articles cited above, including:

1. Policies, procedures, practices, and legal memos relating to the installation and use of port reader processes, devices, hardware, software, or firmware;
2. Technical specifications for the installation and use of port reader processes, devices, hardware, software, or firmware (including any relevant API, ABI, or network protocol specification);
3. What kinds of Internet traffic (i.e., what protocols) are captured by port reader processes, devices, hardware, software, or firmware;
4. What categories of metadata port reader processes, devices, hardware, software, or firmware are capable of capturing, and which categories are in fact collected;
5. Whether and to what extent port readers copy or retain communications content, including any content of emails, any content of instant messages, and any addresses of web pages visited;
6. How many communications have had their content or metadata copied or retained using port reader processes, devices, hardware, software, or firmware;
7. How many individuals have had their communications metadata or content copied or retained using port reader processes, devices, hardware, software, or firmware;
8. Whether telecommunications carriers and Internet service providers have installed port reader processes, devices, hardware, software, or firmware;
9. The case name, docket number, and court of any legal proceeding in which any private entity has challenged or resisted the installation and use of port reader processes, devices, hardware, software, or firmware;
10. Pursuant to which legal authorities the FBI bases its claim that it may lawfully request or compel the installation and/or use of port reader processes, devices, hardware, software or firmware.
11. The name of the tool identified by CNET and *Foreign Policy* as a port reader.

III. Limitation of Processing Fees

The ACLU requests a limitation of processing fees pursuant to 5 U.S.C. § 552(a)(4)(A)(ii)(II) (“fees shall be limited to reasonable standard charges for document duplication when records are not sought for commercial use and the request is made by . . . a representative of the news media . . .”) and 28 C.F.R. §§ 16.11(c)(1)(i), 16.11(d)(1) (search and review fees shall not be charged to “representatives of the news media”). As a representative of the news media, the ACLU fits within this statutory and regulatory mandate. Fees associated with the processing of this request should, therefore, be limited accordingly.

The ACLU meets the definition of a representative of the news media because it is an “entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience.” *Nat’l Sec. Archive v. U.S. Dep’t of Def.*, 880 F.2d 1381, 1387 (D.C. Cir. 1989).

The ACLU is a national organization dedicated to the defense of civil rights and civil liberties. Dissemination of information to the public is a critical and substantial component of the ACLU’s mission and work. Specifically, the ACLU publishes a continuously updated blog, newsletters, news briefings, right-to-know documents, and other educational and informational materials that are broadly disseminated to the public. Such material is widely available to everyone, including individuals, tax-exempt organizations, not-for-profit groups, law students, and faculty, for no cost or for a nominal fee through its public education department and web site. The ACLU web site addresses civil rights and civil liberties issues in depth, provides features on civil rights and civil liberties issues in the news, and contains many thousands of documents relating to the issues on which the ACLU is focused. The website specifically includes features on information obtained through the FOIA.⁶ For example, the ACLU’s “Accountability for Torture FOIA” webpage, <https://www.aclu.org/accountability-torture>, contains commentary about the ACLU’s FOIA request for documents related to the treatment of detainees, press releases, analysis of the FOIA documents disclosed, and an advanced search engine permitting webpage visitors to search the documents obtained through the FOIA. *See Judicial Watch, Inc. v. U.S. Dep’t of Justice*, 133 F. Supp. 2d 52, 53–54 (D.D.C. 2000) (finding Judicial Watch to be a news-media requester because it posted documents obtained through FOIA on its website).

⁶ See, e.g., <https://www.aclu.org/national-security/warrantless-electronic-communications-foia-requests>; <https://www.aclu.org/technology-and-liberty/foia-request-justice-department-policy-memos-gps-location-tracking>; <http://www.aclu.org/national-security/predator-drone-foia>; <http://www.thetorturedatabase.org>; <http://www.aclu.org/mappingthefbi>.

The ACLU maintains and publishes a widely read blog specifically dedicated to covering issues involving “civil liberties in the digital age,”⁷ through which the organization disseminates news and commentary about FOIA requests similar to this one.⁸ The ACLU publishes a newsletter at least twice a year that reports on and analyzes civil-liberties-related current events. The newsletter is distributed to approximately 450,000 people. The ACLU also publishes a bi-weekly electronic newsletter, which is distributed to approximately 300,000 subscribers (both ACLU members and non-members) by e-mail. Both of these newsletters often include descriptions and analyses of information obtained from the government through FOIA, as well as information about cases, governmental policies, pending legislation, abuses of constitutional rights, and polling data. *Cf. Elec. Privacy Info. Ctr. v. Dep’t of Def.*, 241 F. Supp. 2d 5, 13–14 (D.D.C. 2003) (finding the Electronic Privacy Information Center to be a representative of the news media under Department of Defense regulations because it published a “bi-weekly electronic newsletter that is distributed to over 15,000 readers” about “court cases and legal challenges, government policies, legislation, civil rights, surveys and polls, legislation, privacy abuses, international issues, and trends and technological advancements”).

The ACLU also regularly publishes books,⁹ “know your rights” publications,¹⁰ fact sheets,¹¹ and educational brochures and pamphlets designed to educate the public about civil liberties issues and governmental policies that implicate civil rights and liberties. These materials are

⁷ <https://www.aclu.org/blog/free-future>.

⁸ See, e.g., Nathan Freed Wessler, *New Documents Suggest IRS Reads Emails Without a Warrant*, Free Future, (Apr. 10, 2013), <https://www.aclu.org/blog/technology-and-liberty-national-security/new-documents-suggest-irs-reads-emails-without-warrant>.

⁹ Some of the recent books published by the ACLU include: Susan N. Herman, *Taking Liberties: The War on Terror and the Erosion of American Democracy* (Oxford Univ. Press 2011); Lenora M. Lapidus, Emily J. Martin & Namita Luthra, *The Rights of Women: The Authoritative ACLU Guide to Women’s Rights* (NYU Press 4th ed. 2009); Jameel Jaffer & Amrit Singh, *Administration of Torture: A Documentary Record from Washington to Abu Ghraib and Beyond* (Columbia Univ. Press 2007) (a book based on documents obtained through FOIA).

¹⁰ Some of the more recent “know your rights” publications include: ACLU, *Know Your Rights: Pregnant, Post-Partum & Breastfeeding Workers* (Oct. 2013), available at https://www.aclu.org/files/assets/kyr_pregant_breastfeeding.pdf; ACLU, *Know Your Rights: Demonstrations and Protests* (Nov. 2011), available at http://www.aclu.org/files/assets/kyr_protests.pdf; ACLU, *Gender-Based Violence & Harassment: Your School, Your Rights* (May 2011), available at http://www.aclu.org/files/assets/genderbasedviolence_factsheet_0.pdf; ACLU, *Know Your Rights: What to Do If You’re Stopped by Police, Immigration Agents or the FBI* (June 2010), available at http://www.aclu.org/files/assets/bustcard_eng_20100630.pdf.

¹¹ See, e.g., ACLU, *Military Abortion Ban in Cases of Rape and Incest (Factsheet)* (2011), available at <http://www.aclu.org/reproductive-freedom/military-abortion-ban-cases-rape-and-incest-factsheet>; ACLU, *The Facts About “The No Taxpayer Funding For Abortion Act”* (2011), available at http://www.aclu.org/files/assets/Chris_Smith_bill-_ACLU_Fact_Sheet-_UPDATED-4-30-11.pdf.

specifically designed to be educational and widely disseminated to the public. *See Elec. Privacy Info. Ctr.*, 241 F. Supp. 2d at 11 (finding the Electronic Privacy Information Center to be a news-media requester because of its publication and distribution of seven books on privacy, technology, and civil liberties).

Depending on the results of this request, the ACLU plans to “disseminate the information” it receives “among the public” through these kinds of publications in these kinds of channels. The ACLU is therefore a news media entity.

Disclosure is not in the ACLU’s commercial interest. The ACLU is a “non-profit, non-partisan, public interest organization.” *See Judicial Watch Inc. v. Rossotti*, 326 F.3d 1309, 1312 (D.C. Cir. 2003) (“Congress amended FOIA to ensure that it be ‘liberally construed in favor of waivers for noncommercial requesters.’” (citation and internal quotations omitted)). Any information disclosed by the ACLU as a result of this FOIA will be available to the public at no cost.

IV. Waiver of All Costs

The ACLU additionally requests a waiver of all costs pursuant to 5 U.S.C. § 552(a)(4)(A)(iii) (“Documents shall be furnished without any charge . . . if disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester.”).

Disclosure of the requested information will help members of the public understand the privacy risks of using email and other forms of Internet communication. The bulk collection of telephonic metadata and the privacy risks associated with that collection are currently topics of great public interest.¹² The significance of those privacy risks has also been acknowledged, both by a federal judge who ruled that bulk collection of metadata is likely unconstitutional, and by the White House surveillance review board, which recommended that the NSA end bulk collection of

¹² *See, e.g.*, Timothy B. Lee, *Here’s How Phone Metadata Can Reveal Your Affairs, Abortions, and Other Secrets*, Wash. Post, Aug. 27, 2013, <http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/27/heres-how-phone-metadata-can-reveal-your-affairs-abortion-and-other-secrets/>; Charlie Savage, *Judge Questions Legality of N.S.A. Phone Records*, N.Y. Times, Dec. 16, 2013, <http://www.nytimes.com/2013/12/17/us/politics/federal-judge-rules-against-nsa-phone-data-program.html>; Editorial, *NSA’s metadata program: End it, don’t mend it*, L.A. Times, Nov. 5, 2013, <http://articles.latimes.com/2013/nov/05/opinion/la-ed-nsa-feinstein-lahey-sensenbrenner-20131105>.

telephonic metadata.¹³ Meanwhile, the public lacks information about the scale or nature of government collection of email and Internet traffic metadata, which poses similar privacy risks. The requested information will “contribute significantly to public understanding.” 5 U.S.C. § 552(a)(4)(A)(iii).

As a nonprofit 501(c)(3) organization and “representative of the news media” as discussed in Section III, the ACLU is well-situated to disseminate information it gains from this request to the general public and to groups that protect constitutional rights. Because the ACLU meets the test for a fee waiver, fees associated with responding to FOIA requests are regularly waived for the ACLU.¹⁴

Thank you for your prompt attention to this matter. Please furnish all applicable records to:

Catherine Crump
Staff Attorney
American Civil Liberties Union Foundation
125 Broad Street, 17th Floor
New York, NY 10004

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

Sincerely,



Catherine Crump
Staff Attorney
American Civil Liberties Union

¹³ See Ellen Nakashima & Ann Marimow, *Judge: NSA's Collecting of Phone Records is Probably Unconstitutional*, Wash. Post, Dec. 16, 2013, http://www.washingtonpost.com/national/judge-nsas-collecting-of-phone-records-is-likely-unconstitutional/2013/12/16/6e098eda-6688-11e3-a0b9-249bbb34602c_story.html; David E. Sanger & Charlie Savage, *Obama Panel Recommends New Limits on N.S.A. Spying*, N.Y. Times, Dec. 18, 2013, http://www.nytimes.com/2013/12/19/us/politics/report-on-nsa-surveillance-tactics.html?hp&_r=0.

¹⁴ Fees associated with responding to FOIA requests are regularly waived for the ACLU. For example, in May 2012, the Bureau of Prisons granted a fee waiver to the ACLU for a FOIA request seeking documents concerning isolated confinement of prisoners in BOP custody. In March 2012, the Department of Justice Criminal Division granted a fee waiver to the ACLU for a FOIA request seeking records about the government's access to the contents of individuals' private electronic communications. In June 2011, the National Security Division of the Department of Justice granted a fee waiver to the ACLU with respect to a request for documents relating to the interpretation and implementation of a section of the PATRIOT Act.