ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

May 14, 2018

VIA FOIA ONLINE

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

Douglas Hibbard
Chief, Initial Request Staff
Office of Information Policy
Department of Justice
Suite 11050
1425 New York Avenue, N.W.
Washington, DC 20530-0001

VIA EMAIL

Deborah Waller
Government Information Specialist
Office of the Inspector General
Department of Justice
Room 4726
950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001
Email: oigfoia@usdoj.gov

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

To Whom It May Concern:

This letter constitutes an expedited request under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and is submitted to the Federal Bureau of Investigation (FBI), as well as the Office of Information Policy (OIP) at the Department of Justice (DoJ) and the Office of the Inspector General (OIG) at the DoJ. Through this request, EFF seeks records that shed light on statements made by FBI Director Christopher Wray, on what the FBI terms the "Going Dark" problem.

On December 7, 2017, the Committee on the Judiciary of the U.S. House of Representatives held an FBI oversight hearing at which Director Wray presented

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

oral and written testimony on, among other things, what the FBI terms the "Going Dark" problem.[1, 2] Going Dark describes the allegedly increasing difficulties that encryption has posed to the FBI's access to information relevant to its investigations.

Wray, in support of his claims that the FBI has encountered technological difficulties in attempting to access information on encrypted devices, stated:

> In fiscal year 2017, the FBI was unable to access the content of approximately 7800 mobile devices using appropriate and available technical tools, even though there was legal authority to do so. This figure represents slightly over half of all the mobile devices the FBI attempted to access in that timeframe.[3]

On January 9, 2018, Director Wray again spoke about the 'Going Dark' issue at the International Conference on Cybersecurity, held at Fordham University.[4] In his prepared remarks, Director Wray again claimed that the FBI was unable to gain access to thousands of devices by technological means:

> Let me give you some numbers to put some meat on the bones of this problem. In fiscal year 2017, we were unable to access the content of 7,775 devices—using appropriate and available technical tools—even though we had the legal authority to do so. Each one of those nearly 7,800 devices is tied to a specific subject, a specific defendant, a specific victim, a specific threat.[5]

Meanwhile, a March 2018 report from the Department of Justice Office of the Inspector General raises questions about the FBI's handling of an iPhone that

---

[1] *Oversight of the Federal Bureau of Investigation,* House of Representatives Judiciary Committee (December 7, 2017), https://judiciary.house.gov/hearing/oversight-federal-bureau-investigation-2017/.

[2] *Oversight of the FBI: Hearing Before the H. Comm. on the Judiciary,* (statement of Christopher A. Wray, Director, Federal Bureau of Investigation), https://judiciary.house.gov/wp-content/uploads/2017/12/Director-Wray-Testimony.pdf.

[3] *Id.* at 5.

[4] *2018 Program and Schedule,* International Conference on Cyber Security (last accessed May 10, 2018), http://iccs.fordham.edu/iccs2018/.

[5] Christopher Wray, *Raising our Game: Cyber Security in an Age of Digital* Transformation (Remarks prepared for delivery Jan. 9, 2018), https://www.fbi.gov/news/speeches/raising-our-game-cyber-security-in-an-age-of-digital-transformation.

belonged to one of the shooters in the San Bernardino attack.[6] After seeking to a court order to compel Apple to assist the government in unlocking the phone, the FBI instead accessed its contents with the help of an outside party. The OIG report found that that there was inadequate communication within the FBI's Operational Technology Division regarding the FBI's capabilities to gain access to mobile devices, particularly between the Cryptographic and Electronic Analysis Unit (CEAU) and the Remote Operations Unit (ROU).[7]

Recent press reports confirm that third parties, including the companies Cellebrite[8] and Grayshift offer products and services that can unlock even the newest iPhones and that these companies have contracted with law enforcement organizations.[9]

Accordingly, this request seeks any and all records created between January 1, 2015 and the date of this request, that are available to the FBI concerning the FBI's access to encrypted mobile devices in its physical possession, including:

1. All records referring to or referencing the 7,775 mobile devices figure.
2. All records referenced by Director Wray in his statement to Congress on December 7, 2017 relating to the 7,775 mobile devices figure.
3. All records relied upon by Director Wray or any other FBI employee in preparing the 7,775 mobile devices figure.
4. All records describing FBI attempts to gain access to those 7,775 mobile devices.
5. All records relating to when the FBI became aware that an outside entity was either developing or had developed the capability to unlock the iPhone of a suspect of the San Bernardino shooting, or equivalent

---

[6] *Senator reveals that the FBI paid $900,000 to hack into San Bernardino killer's iPhone*, CNBC (May 5, 2017), https://www.cnbc.com/2017/05/05/dianne-feinstein-reveals-fbi-paid-900000-to-hack-into-killers-iphone.html.
[7] *Id*. at 3-4.
[8] Thomas Fox-Brewster, *The Feds Can Now (Probably) Unlock Every iPhone Model in Existence* – UPDATED, Forbes (Feb. 26, 2018), https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/.
[9] Joseph Cox, *Cops Around the Country Can Now Unlock iPhones, Records Show*, Motherboard (Apr. 12, 2018), https://motherboard.vice.com/en_us/article/vbxxxd/unlock-iphone-ios11-graykey-grayshift-police.

models of iPhone, running the same version of its operating system. This includes any specific individuals who were or became aware, and, if applicable, when they became aware.

6. All records relating to statements by Executive Assistant Director Amy Hess relating to the FBI's unlocking of the San Bernardino shooting iPhone, including but not limited to concerns expressed over the accuracy of government officials' statements regarding the San Bernardino shooting iPhone and disagreements within the FBI as to its ability to unlock said iPhone.

7. All records regarding efforts to identify a technical solution to unlocking the San Bernardino shooting iPhone, prior to the FBI's initial filings on February 16, 2016, for an order requiring Apple to aid in unlocking said iPhone.

8. All records of and regarding communications between FBI section chiefs (or other supervisors) and members of their own sections (or other sections) regarding FBI resources that could access information on the San Bernardino shooting iPhone, including but not limited to communications between the CEAU and ROU Chiefs.

9. All records referring to "Grayshift" or "Graykey".

10. All records concerning any briefings, discussions, or other exchanges between FBI officials and members of the Senate or House of Representatives concerning the number of devices that law enforcement is unable to access.

Request for Expedited Processing

For the reasons discussed below, a "compelling need" exists for the records sought in this request. EFF is therefore entitled to expedited processing under 5 U.S.C. § 552(a)(6)(E)(v)(II), 28 C.F.R. §§ 16.5(e)(1)(ii) and (iv).

Expedited Processing under 28 C.F.R. § 16.5(e)(1)(ii)

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 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.

According to the New York Times on March 24, 2018, officials in the Department of Justice have been pushing for legislation to mandate that law enforcement agencies can, with a court order, gain access to information on any mobile device regardless of its technical protections against access.[10] The goal described in that article "gaining "extraordinary access" to encrypted devices," raises urgent issues concerning government intrusions into private communications.[11] As Craig Federighi, Senior Vice President of Software Engineering at Apple, stated in the New York Times, "Proposals that involve giving the keys to customers' device data to anyone but the customer inject new and dangerous weaknesses into product security."[12]

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).

Expedited Processing under 28 C.F.R.§ 16.5(e)(1)(iv).

EFF is also entitled to expedited processing under 28 C.F.R. § 16.5(e)(1)(iv) because the subject of the request concerns "a matter of widespread and exceptional media interest in which there exist possible questions about the government's integrity which affect public confidence."

The Department of Justice Office of the Inspector General's report on the FBI's response to the San Bernardino attack, by its very nature, raise unavoidable concerns about the government's knowledge of its own technical capabilities and the presentation of its capabilities to the public and the justice system, concerns which directly implicate the government's integrity.

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, 28 C.F.R. §§ 16.11(b)(6), (d)(1). In requesting this classification, we note that the Department of Homeland Security has recognized that EFF qualifies as a "news

[10] Charlie Savage, *Justice Dept. Revives Push to Mandate a Way to Unlock Phones*, New York Times (Mar. 24, 2018), https://www.nytimes.com/2018/03/24/us/politics/unlock-phones-encryption.html.
[11] *Id*.
[12] *Id*.

media" requester, based upon the publication activities set forth below (*see* DHS stipulation attached hereto). 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). Furthermore, 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 nonprofit public interest organization dedicated to "defending civil liberties in the digital world."[13] One of EFF's primary objectives is "to educate the general public and foster discussion and public policy analysis regarding the relationship between technology and society."[14] To accomplish this goal, EFF routinely and systematically disseminates information in several ways.

First, EFF maintains a frequently visited web site, https://www.eff.org that reports the latest developments and contains in-depth information about a variety of civil liberties and intellectual property issues. Also, EFF has regularly published an online newsletter, the EFFector, since 1990. The EFFector currently has more than 280,000 subscribers. A complete archive of past EFFectors is available at https://www.eff.org/effector/. Furthermore, EFF publishes a blog, Deeplinks (https://www.eff.org/deeplinks/), that highlights the latest news from around the Internet.

In addition to reporting high-tech developments, EFF staff members have presented research and in-depth analysis on technology issues in roughly 40 white papers published since 2002. These papers, available at https://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

[13] *About EFF*, Electronic Frontier Foundation (last accessed May 10, 2018), https://www.eff.org/about.
[14] *Guidestar Basic Report*, Electronic Frontier Foundation, https://www.guidestar.org/organizations/04-3091431/electronic-frontier-foundation.aspx (last visited Oct. 6, 2015).

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 records and releases videos highlighting important issues relating to surveillance and civil liberties and interviews with EFF staff and outside experts. Many of these videos have been watched hundreds of thousands and even over 1 million times.[15]

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 search 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), 28 C.F.R. §16.11(k)(1). To determine whether a request meets this standard, the regulations require the agency to assess whether "[d]isclosure of the requested information. . . is likely to contribute significantly to public understanding of the operations or activities of the government," 28 C.F.R. § 16.11(k)(1)(i), and whether such disclosure "is not primarily in the commercial interest of the requester." 28 C.F.R. §§ 16.11(k)(1)(i), (ii). EFF's request clearly satisfies these criteria.

First, because FBI is a component of the federal government, any FBI records describing the basis for the agency's stated inability to access 7,775 mobile devices, as well as any records regarding efforts to gain access to the San Bernardino shooting iPhone, would unquestionably document "the operations or activities of the government." 28 C.F.R. §16.11(k)(1)(i).

Second, the requested material will contribute to "public understanding" of the government's activities. 28 C.F.R. § 16.11(k)(2)(iii) (internal quotation marks omitted). EFF has requested information that will lead to greater public understanding of the 'going dark' problem. The requested information is not in the public domain and, therefore, will necessarily contribute to a more robust public understanding of the subject. This information will contribute not only to EFF's understanding, but also to the understanding of a reasonably broad

[15] *See EFForg*, Youtube (last accessed May 10, 2018), https://www.youtube.com/user/EFForg.

audience of persons interested in the subject—including congress members and state and federal judges. EFF will make the information obtained through this request available to the public and the media through its web site and the EFF newsletter, which highlight developments concerning privacy and civil liberties issues. Because EFF is a representative of the news media, EFF's request presumptively satisfies this criterion. *Id.*

Finally, 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)(1)(ii). EFF is a 501(c)(3) nonprofit organization, and will derive no commercial benefit from the information requested here.

Format of Documents

FOIA provides that agency records include records "maintained by an agency in any format, including electronic format." 5 USC § 552(f)(2)(A). FOIA also provides that "an agency shall make reasonable efforts to search for the records in electronic form or format," 5 USC § 552(a)(3)(C), and "shall provide the record in any form or format requested by the person if the record is readily reproducible by the agency in that form or format." 5 USC § 552(a)(3)(B). Accordingly, we request that, where available and appropriate, the requested records be provided in the following manner:

1. That files stored in electronic format be produced in electronic format;

2. That files be produced either in their native format (likely appropriate for spreadsheets and database files – for example, Microsoft Excel files produced as .xls electronic files) or as text-searchable .pdf formatted files (likely appropriate for word processing documents, letters, memos, or emails);

3. That files preserve the "parent / child" relationship between records (for example, if an email has an attachment, that attachment – or, if appropriate, information regarding the attachment's withholding – should accompany or follow the .pdf of the email); and that the beginning and ending of individual records is clearly indicated.

EFF also requests that all pages be consecutively numbered and that the page numbers of pages or records withheld in full be clearly indicated in a document or file accompanying the produced records.

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 ext. 139.

Because EFF has sought expedited processing of this request, I will anticipate a determination of our request for expedited processing within 10 calendar days, and a determination with respect to the disclosure of requested records within 20 working days. If you have any questions or concerns, do not hesitate to contact me at michael.rosenbloom@eff.org or 415-436-9333 x 139.

Sincerely,

Michael Rosenbloom
Legal Fellow
Electronic Frontier Foundation
michael.rosenbloom@eff.org

Andrew Crocker
Staff Attorney
Electronic Frontier Foundation
andrew@eff.org

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. DEPARTMENT OF HOMELAND SECURITY, Defendant.	)	Civil Action No. 06-1988 (ESH)

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.

/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

(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,

for Marianne Stupar

PAMELA N. PHILLIPS
Chief
FOIA/PA Office