Stanford Law School

Riana Pfefferkorn
Cryptography Fellow
Stanford Center for Internet and Society
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610
riana@law.stanford.edu

April 11, 2016

FOIA/PA Mail Referral Unit
Department of Justice
Room 115
LOC Building
Washington, DC 20530-0001
Email: MRUFOIA.Requests@usdoj.gov

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

Ken Courter
Chief, FOIA/PA Unit
Criminal Division
Department of Justice
Suite 1127, Keeney Building
950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001
Email: crm.foia@usdoj.gov

Arnetta Mallory
FOIA Initiatives Coordinator
National Security Division
Department of Justice
Room 6150
950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001
E-mail: nsdfoia@usdoj.gov

Susan B. Gerson
Assistant Director, FOIA/Privacy Unit
Executive Office for United States Attorneys
Department of Justice
Room 7300, 600 E Street, N.W.
Washington, DC 20530-0001
Email: USAEO.FOIA.Requests@usdoj.gov

Melissa Golden
Lead Paralegal and FOIA Specialist
Office of Legal Counsel
Department of Justice
Room 5511, 950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001
E-mail: usdoj-officeoflegalcounsel@usdoj.gov

Re: FREEDOM OF INFORMATION ACT REQUEST

To Whom It May Concern:

Under the Freedom of Information Act, the Stanford Center for Internet and Society ("CIS") hereby requests the disclosure of records, as specified below, regarding the imposition of encryption-related technical-assistance requirements on mobile device manufacturers, mobile operating system developers, Internet communications providers, and other third parties.

I. The Requested Records

CIS seeks disclosure of the following records:

1. Any policies, guidance, memoranda, manuals, directives, correspondence, briefs, minutes, notes, or any other records, including any drafts of same, created on or after September 11, 2001, that interpret, analyze, or explain any of the following statutes and regulations (hereafter, collectively, the "Technical-Assistance Laws"), either singly or in connection with any other Technical-Assistance Law(s):

    a. 28 U.S.C. § 1651(a) (the "All Writs Act" or "AWA");
    b. 18 U.S.C. §§ 2511(2)(a)(ii), 2518(4), or 2522 (collectively, the "Wiretap Act");
    c. 18 U.S.C. § 2703(d) (the "Stored Communications Act" or "SCA");
    d. 18 U.S.C. §§ 3123(b)(2) or 3124(a) or (b) (collectively, the "Pen/Trap Act");
    e. 50 U.S.C. § 1881a(h) (the "FISA");
    f. Federal Rule of Criminal Procedure 41, in connection with encryption-related assistance (as that term is defined in number 5 below);
    g. 47 U.S.C. §§ 1001(4), 1001(6), 1001(8), 1002, or 1007, 20 F.C.C. Rcd. 14989 (2005), or 21 F.C.C. Rcd. 5360 (2006) (collectively, "CALEA").

2. Any policies, guidance, memoranda, manuals, directives, correspondence, briefs, minutes, notes, or any other records, including any drafts of same, created on or after September 11, 2001, that address the legal interpretation of the following cases: *United States v. New York Telephone Co.*, 434 U.S. 159 (1977); *Pennsylvania Bureau of Correction v. United States Marshals Service*, 474 U.S. 34 (1985); *Bank of U.S. v. Halstead*, 23 U.S. (10 Wheat.) 51 (1825); *In re Application of United States for an Order Authorizing an In-Progress Trace of Wire Communications over Telephone Facilities (Mountain Bell)*, 616 F.2d 1122 (9th Cir. 1980).

3. Any policies, guidance, memoranda, manuals, directives, correspondence, briefs, minutes, notes, or any other records, including any drafts of same, created on or after September 11, 2001, that relate to the applicability of any of the Technical-Assistance Laws, or any of the cases listed in number 2 above, to manufacturers of mobile devices (including without limitation Apple, HTC, Huawei, Lenovo, LG, Motorola, Nokia, Samsung, Sony, and ZTE);

4. Any policies, guidance, memoranda, manuals, directives, correspondence, briefs, minutes, notes, or any other records, including any drafts of same, created on or after September 11, 2001, that relate to the applicability of any of the Technical-Assistance Laws, or any of the cases listed in number 2 above, to developers of operating systems for mobile devices (including without limitation Apple, BlackBerry [Research in Motion], Google [Android, Inc.], HP [Hewlett-Packard], Microsoft, Mozilla, and Symbian);

5. Any policies, guidance, memoranda, manuals, directives, correspondence, briefs, minutes, notes, or any other records, including any drafts of same, created on or after September 11, 2001, that discuss whether any of the Technical-Assistance Laws, or any of the cases listed in number 2 above, authorize an order or other authorization requiring a mobile device manufacturer, mobile operating system developer, service

provider,[1] Internet communications providers, or other third party,[2] to provide any of the following assistance (hereafter "encryption-related assistance"): decrypt a device, data, or communications; provide the government with the ability, facilities, or information necessary to decrypt a device, data, or communications (including encryption keys and Secure Socket Layer [SSL] keys); circumvent or bypass the encryption, passcode, or passphrase of a device, data, or communications; alter the design of an encryption algorithm; insert a "backdoor" into an encryption algorithm; use a different encryption algorithm; or cease use of an encryption algorithm;

6. Any policies, guidance, memoranda, manuals, directives, correspondence, briefs, minutes, notes, or any other records, including any drafts of same, created on or after September 11, 2001, that address the circumstances in which the Department of Justice (including any component thereof and any Government attorney) should, may, or will, or should not, may not, or will not, seek a court order or other authorization under any of the Technical-Assistance Laws to compel the furnishing of technological assistance by a mobile device manufacturer, mobile operating system developer, Internet service/communications provider, or other third party;

7. Any policies, guidance, memoranda, manuals, directives, correspondence, briefs, minutes, notes, or any other records, including any drafts of same, created on or after September 11, 2001, that address the process, protocol, or procedure by which the Department of Justice (including any component thereof and any Government attorney) should seek, and if obtained implement, a court order or other authorization under any of the Technical-Assistance Laws to compel the furnishing of encryption-related assistance by a mobile device manufacturer, mobile operating system developer, service provider, or other third party;

8. Any sample or form language, subpoena, warrant, affidavit, declaration, application, brief, memorandum of points and authorities, attachment, order, proposed order, authorization, letter, or consent form relating to the furnishing of encryption-related assistance by a mobile device manufacturer (including without limitation those listed in number 3 above), mobile operating system developer (including without limitation those listed in number 4 above), service provider, or other third party under any of the Technical-Assistance Laws, whether or not such sample or form was ultimately adopted, approved, circulated, or otherwise made available internally or externally;

9. Any and all requests or applications submitted to any federal judge since September 11, 2001, seeking a warrant, court order, or other authorization under any of the Technical-Assistance Laws to compel the furnishing of encryption-related assistance by a mobile device manufacturer (including without limitation those listed in number 3 above), mobile operating system developer (including without limitation those listed in number 4 above), service provider, or other third party, as well as any and all affidavits, declarations, briefs, memoranda of points and authorities, attachments, proposed orders, or other materials submitted with each such request or application;

10. Any and all warrants, orders, or other authorizations issued by any judge pursuant to or in response to the requests and applications listed in number 9 above, including any orders that do not grant the request or application;

11. Any and all requests or demands submitted since September 11, 2001, to a mobile device manufacturer (including without limitation those listed in number 3 above), mobile operating system developer

[1] As used in this FOIA request, "service provider" includes telecommunications carriers as defined in 47 U.S.C. § 1001(8), as well as providers of (1) wire communication services as defined in 18 U.S.C. § 2510(1), (2) electronic communication services as defined in 18 U.S.C. § 2510(15), (3) remote computing services as defined in 18 U.S.C. § 2711(2), (4) electronic messaging services as defined in 47 U.S.C. § 1001(4), and (5) information services as defined in 47 U.S.C. § 1001(6).

[2] As used in this FOIA request, "other third party" includes without limitation a "landlord," "custodian," or "other person" as used in 18 U.S.C. §§ 2518(4) and 3124.

(including without limitation those listed in number 4 above), service provider, or other third party, for the furnishing of encryption-related assistance, regardless of the legal authority, if any, on which such request or demand was based, and including requests for voluntary encryption-related assistance.

CIS requests that responsive electronic records be provided electronically in their native file format.[3] If this FOIA request is denied in whole or in part, CIS requests disclosure of the reasons for each denial, pursuant to 5 U.S.C. § 552(a)(6)(A)(i). In addition, CIS requests release of all segregable portions of otherwise exempt material, in accordance with 5 U.S.C. § 552(b).

II. Expedited Processing

CIS requests expedited processing pursuant to 5 U.S.C. § 552(a)(6)(E). There is a "compelling need" for expeditious disclosure because the documents requested are urgently needed by an organization primarily engaged in disseminating information in order to inform the public about actual or alleged government activity.[4] In addition, there is an "urgency to inform the public" concerning the requested records.[5]

A. CIS is an organization primarily engaged in disseminating information in order to inform the public about actual or alleged government activity.

CIS is "primarily engaged in disseminating information" within the meaning of the statute and regulations.[6]

CIS is a public interest technology law and policy program at Stanford Law School and a part of the Law, Science and Technology Program at Stanford Law School. Founded in 2000, CIS studies the interaction of technology and the law and examines how that dynamic can either promote or harm public goods such as privacy, free speech, innovation, and scientific inquiry. CIS provides law students and the general public with educational resources and analyses of policy issues arising at the intersection of law, technology, and the public interest. CIS also sponsors a range of public events, including a speaker series, conferences, and workshops.[7]

Dissemination of information about actual or alleged government activity is a key component of CIS's work. CIS has dedicated staff specifically responsible for researching government activity in the area of encryption law and policy, such as the government's legal theories, policies, and practices regarding encryption-related third-party technical assistance that are the subject of this Request.[8] CIS disseminates information to the public through its website[9]; posts on Just Security,[10] an online forum for the rigorous

[3] *See* 5 U.S.C. § 552(a)(3)(B).

[4] 5 U.S.C. § 552(a)(6)(E)(v).

[5] 28 C.F.R. § 16.5(e)(1)(ii); *Open Am. v. Watergate Spec. Prosec. Force*, 547 F.2d 605, 614 (D.C. Cir. 1976) (recognizing right of expedition).

[6] 5 U.S.C. § 552(a)(6)(E)(v)(II); *see ACLU v. Dep't of Justice*, 321 F. Supp. 2d 24, 30 n.5 (D.D.C. 2004) (finding that a non-profit, public-interest group that "gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw material into a distinct work, and distributes that work to an audience" is "primarily engaged in disseminating information") (internal citation omitted); *see also Leadership Conference on Civil Rights v. Gonzales*, 404 F. Supp. 2d 246, 260 (D.D.C. 2005) (finding Leadership Conference—whose mission is "to serve as the site of record for relevant and up-to-the-minute civil rights news and information" and to "disseminate[] information regarding civil rights and voting rights to educate the public [and] promote effective civil rights laws"—to be "primarily engaged in the dissemination of information").

[7] Center for Internet and Society: About Us, https://cyberlaw.stanford.edu/about-us (last visited Apr. 11, 2016).

[8] Jennifer Granick, *Federal Judge Shines a Spotlight on the "Going Dark" Debate*, Center for Internet and Society (Oct. 14, 2015), https://cyberlaw.stanford.edu/blog/2015/10/federal-judge-shines-spotlight-%E2%80%9Cgoing-dark%E2%80%9D-debate.

[9] Blog, Center for Internet and Society, https://cyberlaw.stanford.edu/blog (last visited Apr. 11, 2016).

analysis of U.S. national security law and policy, as well as other blogs; news interviews[11]; speeches at other law schools[12]; and publications including white papers, books, and academic writing.[13] CIS disseminates this information to educate the public and to encourage decision makers in the public and private sectors to further democratic values in the design of new laws and new technologies.

CIS plans to analyze and disseminate to the public the information gathered through this Request. The records requested are not sought for commercial use, and CIS plans to disseminate the information disclosed as a result of this Request to the public at no cost.

B. The records sought are urgently needed to inform the public about actual or alleged government activity.

These records are urgently needed to inform the public about actual or alleged government activity, as demonstrated by numerous articles that have been published on the subject of that activity.[14]

Whether and when the government should have the authority to compel technology companies to provide law enforcement with assistance to access encrypted user data is a matter of increasing public concern and national media attention.

The government has in the past compelled a third-party encrypted email service provider, Lavabit, to turn over its encryption keys.[15] The Lavabit case was closely watched because it could have decided the future

---

[10] *E.g.*, Jennifer Granick & Riana Pfefferkorn, *Update on Apple's Compelled-Decryption Case*, Just Security (Oct. 20, 2015), https://www.justsecurity.org/26964/update-apples-compelled-decryption-case/; Jennifer Granick & Riana Pfefferkorn, *The All Writs Act, Software Licenses, and Why Judges Should Ask More Questions*, Just Security (Oct. 26, 2015), https://www.justsecurity.org/27109/writs-act-software-licenses-judges-questions/; Jennifer Granick & Riana Pfefferkorn, *A Quick Update: Apple, Privacy, and the All Writs Act of 1789*, Just Security (Oct. 30, 2015), https://www.justsecurity.org/27214/quick-update-apple-privacy-writs-act-1789/; Jennifer Granick, *Who Sets the Rules of the Privacy and Security Game?*, Just Security (Feb. 22, 2016), https://www.justsecurity.org/29446/sets-rules-privacy-security-game/.

[11] *E.g.*, Aarti Shahani, *Phone Carriers Tight-Lipped On How They Will Comply with New Surveillance Law*, National Public Radio (June 8, 2015), http://www.npr.org/sections/alltechconsidered/2015/06/04/411870819/phone-carriers-are-tight-lipped-over-law-that-overhauls-nsa-surveillance (CIS Director of Civil Liberties Jennifer Granick interviewed for news radio show about phone companies' obligations under the newly-enacted USA Freedom Act); Joel Rose, *The Seeds of Apple's Standoff with DOJ May Have Been Sown in Brooklyn*, National Public Radio (Feb. 22, 2016), http://www.npr.org/2016/02/22/467602161/the-seeds-of-apples-standoff-with-doj-may-have-been-sown-in-brooklyn (Jennifer Granick interviewed for news radio show about DOJ cases seeking to compel Apple's assistance in accessing encrypted iPhone data in New York and California).

[12] *See, e.g.*, Jennifer Granick presentation at U.C. Davis Law School, "Bye Bye, American Spies" (Jan. 13, 2015), discussing U.S. government role in undermining global encryption standards, intercepting Internet companies' data center transmissions, using auto-update to spread malware, and demanding law enforcement back doors in products and services, announcement available at http://performancestudies.ucdavis.edu/2015/01/06/digitalculturesnews-jennifer-granick-esq-bye-bye-american-spies-on-january-13th/; Riana Pfefferkorn presentation at U.C. Berkeley Law School, "Apple vs. the FBI: Where Does It Come From? What Is It? Where Is It Going?" (Mar. 7, 2016), discussing the 1990s "crypto wars" and New York and California DOJ cases seeking access to encrypted iPhones, announcement available at http://ems.law.berkeley.edu/MasterCalendar/EventDetails.aspx?data=hHr80o3M7J6OJPasRboqq1ZAt%2FeEQeDqFyKAo7CFf2CrRCoTwd3DD%2FDbbP%2B9Gzkh.

[13] *E.g.*, Barbara van Schewick & Morgan N. Weiland, *New Republican Bill is Network Neutrality in Name Only*, 67 Stan. L. Rev. Online 85 (Jan. 20, 2015), http://www.stanfordlawreview.org/online/new-republican-bill-is-network-neutrality-in-name-only (analyzing draft bill in the U.S. Congress about regulation of Internet service providers); *see generally* Publications, Center for Internet and Society, https://cyberlaw.stanford.edu/publications.

[14] *See* 28 C.F.R. § 16.5(e)(3) ("The existence of numerous articles published on a given subject can be helpful in establishing the requirement that there be an 'urgency to inform' the public on the topic.").

[15] *See In re Under Seal (Lavabit)*, 749 F.3d 276, 282-84 (4th Cir. 2014) (government obtained seizure warrant for "all information necessary to decrypt communications sent to or from [the target's] Lavabit email account ..., including encryption keys and SSL keys"; government asserted four different legal bases for why Lavabit was required to produce the encryption keys to law enforcement).

reliability of encryption protocols to protect all Internet communications. The Department of Justice had issued an order under the Pen/Trap Act demanding that Lavabit capture transactional data related to one of its e-mail customers, recently revealed to be NSA whistleblower Edward Snowden. Lavabit's owner, Ladar Levison, told the government that the information was encrypted. At that point, the government tried multiple legal tools purporting to compel Lavabit to disclose its encryption keys to the government. Specifically, the government got a seizure warrant from the district court under the Stored Communications Act ("SCA") and claimed that the pen/trap order and the SCA order entitled it to take possession of Lavabit's encryption keys. On appeal, the Fourth Circuit realized disclosure of the encryption keys would expose communications data for all of Lavabit's 400,000 customers. But the Fourth Circuit did not reach the issue of whether the key seizure demand was lawful because the issues had not been adequately preserved below. It remains an open question whether and when the government can compel key disclosure.

Nevertheless, news reports suggest that the government may have compelled the furnishing of encryption keys in other, sealed cases, without publicly clarifying the purported legal authority.[16]

The contentious policy debate surrounding device encryption, law enforcement access, and compelled third-party assistance has been growing for at least the past year and a half.[17] A federal judge in Brooklyn added to the technical assistance debate last October by publicizing the government's request to compel Apple to unlock a locked iPhone.[18] The debate has reached fever pitch since mid-February, when the government obtained an order (since vacated) compelling Apple to write new software code to let law enforcement try to access an encrypted iPhone used by one of the San Bernardino shooters.[19] That case has

---

[16] *See* Zack Whittaker, *US Government Pushed Tech Firms to Hand over Source Code*, ZDNet (Mar. 17, 2016), http://www.zdnet.com/article/us-government-pushed-tech-firms-to-hand-over-source-code/.

[17] *See* Danny Yadron, *U.S. Cites Aged Law to Decrypt Phone Data*, Wall St. J. (Nov. 27, 2014), http://www.wsj.com/articles/u-s-cites-aged-law-to-decrypt-phone-data-1417131617; Craig Timberg and Greg Miller, *FBI Blasts Apple, Google for Locking Police Out of Phones*, Wash. Post (Sept. 25, 2014), https://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html.

[18] *See, e.g.*, Cyrus Farivar, *Feds: New Judge Must Force iPhone Unlock, Overturning Ruling That Favored Apple*, Ars Technica (Mar. 7, 2016), http://arstechnica.com/tech-policy/2016/03/feds-new-judge-must-force-iphone-unlock-overturning-ruling-that-favored-apple/; Ellen Nakashima, *Judge Rules in Favor of Apple in Key Case Involving a Locked iPhone*, Wash. Post (Feb. 29, 2016), https://www.washingtonpost.com/world/national-security/judge-rules-in-favor-of-apple-in-key-case-involving-a-locked-iphone/2016/02/29/fa76783e-db3d-11e5-925f-1d10062cc82d_story.html; Cyrus Farivar, *Faced With an iPhone They Can't Unlock, Cops Again Turn to Apple for Help*, Ars Technica (Oct. 21, 2015), http://arstechnica.com/tech-policy/2015/10/judge-does-us-law-allow-feds-to-compel-apple-to-unlock-an-iphone/; Sarah Jeong, *The Obscure 1789 Statute that Could Force Apple to Unlock a Smartphone*, Vice: Motherboard (Oct. 13, 2015), http://motherboard.vice.com/read/writs-and-giggles; Ellen Nakashima, *With Court Order, Federal Judge Seeks to Fuel Debate about Data Encryption*, Wash. Post (Oct. 10, 2015), https://www.washingtonpost.com/world/national-security/federal-judge-stokes-debate-about-data-encryption/2015/10/10/c75da20e-6f6f-11e5-9bfe-e59f5e244f92_story.html; John Riley, *Judge Declines to Order Apple to Disable Security on Device Seized By U.S.*, Newsday (Oct. 9, 2015); http://www.newsday.com/news/new-york/federal-jurist-won-t-force-apple-to-disable-security-on-device-seized-by-u-s-1.10943147.

[19] *See, e.g.*, Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks*, Wash. Post (Feb. 17, 2016), https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html; Eric Lichtblau and Katie Benner, *Apple Fights Order to Unlock San Bernardino Gunman's iPhone*, N.Y. Times (Feb. 17, 2016), http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html; Daisuke Wakabayashi, *Apple Opposes Judge's Order to Help Unlock Phone Linked to San Bernardino Attack*, Wall St. J. (Feb. 17, 2016), http://www.wsj.com/articles/apple-to-oppose-judge-order-to-help-unlock-phone-linked-to-san-bernardino-attack-1455698783; *see also* Russell Brandom, *FBI and Apple Take iPhone Battle to House Committee Hearing*, The Verge (Mar. 1, 2016), http://www.theverge.com/2016/3/1/11139636/fbi-apple-encryption-testimony-house-judiciary-committee (reporting on House Judiciary Committee hearing regarding Riverside case, including testimony from Apple's general counsel and the head of the FBI).

sparked additional discussion of whether compelling such access is within the courts' authority to decide, or a decision properly left to the political branch of government.[20]

The full extent of the government's efforts to require third parties to provide technical assistance to bypass encryption is still unknown even though the government has apparently compelled such assistance on dozens of occasions, largely in sealed proceedings.[21] Nor has the government publicized its legal rationale for why such assistance may be compelled until called upon to do so in these two high-profile cases. However, the government has been obtaining All Writs Act orders under seal even while publicly advocating for legislation to outlaw device encryption that is inaccessible by law enforcement.[22] The government's reliance on the All Writs Act in so many cases across the country, even while it publicly recognized the absence of any on-point statutory authority, indicates that the DOJ has internally considered the question of what legal authority it can use to obtain these orders. The AWA, the Wiretap Act, the Pen/Trap Act, the Stored Communications Act, and other Technical-Assistance Laws are the most likely candidates for analysis. As the debate over law enforcement's proper powers continues, the public has the right to know the government's interpretation of how the nation's laws authorize the powers it asserts.

The government's legal basis for, and history of, forcing third parties to assist in accessing encrypted devices and communications should not be shrouded in secrecy. The lack of transparency with respect to such access is all the more troubling because of the disputed nature of the authority that is provided by the All Writs Act[23] and foreclosed by the Communications Assistance for Law Enforcement Act.[24]

Expedited release of the requested records is necessary to allow the public to better understand the conditions and legal rationale under which the government has compelled or believes it can compel third

---

[20] *See, e.g.*, Dustin Volz, *Judicial Panel Members Consider Legal Brief in Apple Case: Sources*, Reuters (Feb. 29, 2016), http://www.reuters.com/article/us-apple-encryption-amici-idUSKCN0W32WA (reporting that House Judiciary Committee members were considering filing an *amicus curiae* brief in Riverside case to "argue that the case should be decided by Congress and not the courts"; ultimately, no brief was filed); Katie Benner, Eric Lichtblau, and Nick Wingfield, *Apple Goes to Court, and F.B.I. Presses Congress to Settle iPhone Privacy Fight*, N.Y. Times (Feb. 25, 2016), http://www.nytimes.com/2016/02/26/technology/apple-unlock-iphone-fbi-san-bernardino-brief.html (reporting that both the FBI and Apple wanted Congress, not the courts, to decide iPhone encryption issue).

[21] During a court hearing held in the Brooklyn case on October 26, 2015, the government indicated there were at least 70 cases as of that time in which it has applied for and obtained an order under the All Writs Act alone to compel a third party to unlock a mobile device. Transcript of Oral Argument at 24, *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued By this Court* (*In re Order*), No. 1:15-mc-01902-JO (Oct. 26, 2015). Since then, the government has sought at least a dozen more orders to Apple just under the All Writs Act alone. *See* Devlin Barrett, *Justice Department Seeks to Force Apple to Extract Data from About 12 Other iPhones*, Wall St. J. (Feb. 23, 2016), http://www.wsj.com/articles/justice-department-seeks-to-force-apple-to-extract-data-from-about-12-other-iphones-1456202213.

[22] *See, e.g.*, Sam Sacks, *FBI Director Continues Crusade Against Encryption, Calls on Congress to Act*, The District Sentinel (Mar. 25, 2015), https://www.districtsentinel.com/fbi-director-continues-crusade-against-encryption-calls-on-congress-to-act/; Lauren Walker, *FBI's Comey Calls for Making Impenetrable Devices Unlawful*, Newsweek (Oct. 18, 2014), http://www.newsweek.com/going-not-so-bright-fbi-director-james-comey-calls-making-impenetrable-devices-278190.

[23] Civil liberties advocates have argued that the All Writs Act does not provide the authority to compel a third party to bypass device encryption at the behest of law enforcement. *See, e.g.*, Andrew Crocker, *Sifting Fact from Fiction with All Writs and Encryption: No Backdoors*, EFF: Deeplinks Blog (Dec. 3, 2014), https://www.eff.org/deeplinks/2014/12/sifting-fact-fiction-all-writs-and-encryption-no-backdoors ("Simply put, the government cannot use an authority like the All Writs Act to force a company to backdoor its product.").

[24] *See* 47 U.S.C. § 1002(b)(3) (precluding CALEA covered entities from responsibility for decrypting or ensuring government ability to decrypt encrypted communications except in narrow specified circumstances); Matthew Braga, *The FBI Is at War with Apple Because It Couldn't Change Wiretap Law*, Vice: Motherboard (Mar. 1, 2016), https://motherboard.vice.com/read/calea-my-old-friend (quoting CIS Director of Privacy Al Gidari's analysis that CALEA precludes courts from compelling the encryption-related technical assistance sought by DOJ in California case involving encrypted iPhone).

parties to provide access to otherwise encrypted data. In addition, expedited release will allow Americans to learn how the government has interpreted or invoked potentially relevant legal authorities to gain such access.

III. Limitation of Processing Fees

CIS requests a limitation of processing fees pursuant to 5 U.S.C. § 552(a)(4)(A)(ii)(II). As an educational institution, CIS fits within this statutory mandate. Fees associated with the processing of this request should, therefore, be limited accordingly.

As part of Stanford Law School, CIS qualifies as an "educational institution" as defined by Section 552 of the FOIA and its implementing regulations.[25] As required by applicable regulations, CIS's Request (1) "is authorized by, and is made under the auspices of, an educational institution"; (2) seeks records "not … for a commercial use, but rather … to further scholarly research"; and (3) "serve[s] the scholarly research goals of the institution rather than an individual research goal."[26] CIS seeks the requested records in furtherance of CIS's institutional research goals, namely its research project pertaining to the government's policies, practices, and legal rationale for compelling third parties to provide access to otherwise encrypted data. CIS has funding from Stanford University's Cyber Initiative earmarked specifically for this research,[27] has dedicated staff to perform this research,[28] has published repeatedly on this topic,[29] recently filed an *amicus curiae* brief in the high-profile California court case addressing this topic,[30] and plans to publish academic white papers and/or law review articles to analyze and disseminate to the public the information it receives through this Request. CIS's Request is therefore entitled to limitation of processing fees.[31]

Disclosure is not in CIS's commercial interest. CIS is part of Stanford University, a nonprofit 501(c)(3) educational institution.[32] Any information disclosed by CIS as a result of this FOIA will be available to the public at no cost.

IV. Waiver of Costs

CIS also requests a waiver of all search, review, or duplication fees on the ground that disclosure of the requested information is in the public interest because it is "likely to contribute significantly to public

---

[25] 5 U.S.C. § 552(a)(4)(A)(ii)(II) (requiring processing fee limitation for records sought for non-commercial use and requested by "an educational … institution, whose purpose is scholarly … research"); 28 C.F.R. § 16.10(b)(4) (Department of Justice regulation defining "educational institution" as "any school that operates a program of scholarly research" for purposes of FOIA request processing fees); *see Nat'l Sec. Archive v. Dep't of Defense*, 880 F.2d 1381, 1383-84 (D.C. Cir. 1989) (concluding that Congress intended the phrase "educational institution" in Section 552(a)(4)(A) to be given "the ordinary meaning of that term," that is, "school").

[26] 28 C.F.R. § 16.10(b)(4).

[27] *See* Funded Research Projects, Stanford Cyber Initiative, https://cyber.stanford.edu/research-and-publications/funded-research-projects (last visited Apr. 11, 2016) (listing interdisciplinary research project on U.S. cryptography law and policy, co-headed by CIS Director of Civil Liberties Jennifer Granick).

[28] *See supra* n.8.

[29] *See supra* nn.8, 9.

[30] *See* Riana Pfefferkorn, *CIS Files Amici Curiae Brief in Apple Case on Behalf of iPhone Security Experts and Applied Cryptographers*, Center for Internet and Society (Mar. 2, 2016), https://cyberlaw.stanford.edu/blog/2016/03/cis-files-amici-curiae-brief-apple-case-behalf-iphone-security-experts-and-applied (linking to PDF of brief).

[31] 5 U.S.C. § 552(a)(4)(A)(ii)(II); 28 C.F.R. § 16.10(c)(1)(i), (d)(1) (Department of Justice regulations exempting from search fees requests by educational institutions and representatives of the news media).

[32] Stanford Legal Facts, Office of the General Counsel, Stanford University, https://ogc.stanford.edu/stanford-legal-facts (last visited Apr. 11, 2016).

understanding of the operations or activities of the government," and it is "not primarily in the commercial interest of the requester."[33] This request clearly satisfies these criteria.

There can be no doubt that the subject of the request is of significant interest to the American public. As discussed above, the California iPhone case was national news from mid-February of this year until its conclusion at the end of March, amplifying the already considerable debate that was stoked by the Brooklyn iPhone case and has been ongoing since the fall of 2014. Yet the government's interpretation and use of the Technical-Assistance Laws has been largely opaque. Its use of sealed orders and unclear statutory authority circumvents an ongoing and heated public debate on whether the government should be able to compel technology companies to provide access to encrypted data, and which branch of our tripartite government is the appropriate arbiter of that question. The government's reliance on the All Writs Act in over 70 device-encryption cases, the contested scope of that Act's authority, the potential impact of CALEA on same, and the government's past use of the Pen/Trap Act and the Stored Communications Act in at least one case involving encrypted communications, all suggest that the government has internally debated what authorities are available to it to compel third parties to provide access to encrypted data. It further suggests the government has consequently developed a policy and practice based on that analysis, which it has been employing in obtaining court orders. All of this has occurred largely in secret, without public scrutiny. This conduct is of particular concern because the government is relying on contested interpretations of the All Writs Act and CALEA to gain this access, even though Congress has not passed any law squarely authorizing it.

The Request satisfies all of the considerations set forth in the applicable regulation for deciding whether "requested information is in the public interest because it is likely to contribute significantly to public understanding of operations or activities of the government."[34] CIS seeks records that pertain directly to federal government activities.[35] Because the requested records are either documents internal to the DOJ, documents submitted by the DOJ to private third parties, or court documents that are likely scattered across various courts and under seal, disclosure would significantly enhance public understanding of government policies and practices apparently developed in secret without public scrutiny.[36] Due to their relevance to the ongoing policy debate, the records would be of interest to a broad audience, including legal scholars, organizations that protect constitutional rights, other members of the news media, and the public at large.[37]

As part of a 501(c)(3) nonprofit educational institution, CIS does not have a commercial interest in the disclosure of the requested records. CIS plans to disseminate the records received in response to this Request to law students, legal scholars, civil liberties organizations, and the general public, through methods including its website,[38] blog posts, and academic publications such as white papers and/or law review articles.[39]

Pursuant to applicable statute and regulations, we expect a determination regarding expedited processing within ten (10) calendar days of your receipt of this Request.[40]

If the request is denied in whole or in part, we ask that you justify all withholdings by reference to specific exemptions to the FOIA. We also ask that you release all segregable portions of otherwise exempt material.

---

[33] 5 U.S.C. § 552(a)(4)(A)(iii); *see also* 28 C.F.R. § 16.10(k)(1).

[34] 28 C.F.R. § 16.10(k)(2).

[35] *See* 28 C.F.R. § 16.10(k)(2)(i).

[36] *See* 28 C.F.R. § 16.10(k)(2)(ii), (iv).

[37] *See* 28 C.F.R. § 16.10(k)(2)(iii) (noting that representatives of the news media presumptively satisfy this factor).

[38] A requester's dissemination of information obtained through FOIA requests primarily or exclusively online rather than through traditional print outlets does not disqualify a request from a public-interest waiver. *See Cause of Action v. Fed. Trade Comm'n*, 799 F.3d 1108, 1117 (D.C. Cir. 2015) ("[S]urely a newspaper is not disqualified if it forsakes newsprint for (or never had anything but) a website.").

[39] 28 C.F.R. § 16.10(k)(1).

[40] *See* 5 U.S.C. § 552(a)(6)(E)(ii)(I); 28 C.F.R. § 16.5(e)(4).

We reserve the right to appeal a decision to withhold any information or to deny expedited processing or a waiver of fees.

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

Stanford Center for Internet and Society
559 Nathan Abbott Way
Stanford, CA 94305
Fax: (650) 725-4086
riana@law.stanford.edu
jennifer@law.stanford.edu

I certify that the foregoing is true and correct.

Sincerely,

Riana Pfefferkorn

Riana Pfefferkorn
Stanford Center for Internet and Society
559 Nathan Abbott Way
Stanford, CA 94305
Tel: (650) 721-1491
Fax: (650) 725-4086
riana@law.stanford.edu