



May 24, 2018

Deborah M. Waller
Government Information Specialist
Office of the Inspector General
Office of General Counsel
950 Pennsylvania Ave., N.W.
Room 4726
Washington, D.C. 20530
Tel: 202-616-0646
Fax: 202-616-9152

Laurie Day
Chief, Initial Request Staff
Office of Attorney General
c/o Office of Information Policy
Department of Justice
Suite 11050
1425 New York Avenue, N.W.
Washington, D.C. 20530-0001
Tel: (202) 514-FOIA
Fax: (202) 514-1009

Federal Bureau of Investigation
Attn: FOI/PA Request
Record/Information Dissemination Section
170 Marcel Drive
Winchester, VA 22602-4843
Fax: 540-868-4391/4997

**Re: Request Under Freedom of Information Act
(Expedited Processing & Fee Waiver Requested)**

To Whom It May Concern:

The American Civil Liberties Union and the American Civil Liberties Union Foundation (together, the “ACLU”)¹ submit this Freedom of Information

¹ The American Civil Liberties Union Foundation is a 26 U.S.C. § 501(c)(3) organization that provides legal representation free of charge to individuals and organizations in civil rights and civil liberties cases, educates the public about civil rights and civil liberties issues across the country, directly lobbies legislators, and mobilizes the American Civil Liberties Union’s

Act (“FOIA”) request (the “Request”) for records pertaining to any policies of the Department of Justice (“DOJ”) requiring approval from the Deputy Attorney General in order for the Federal Bureau of Investigation (“FBI”) to use classified techniques in criminal cases and any examples of the involvement of the FBI’s Remote Operations Unit (“ROU”) engaging in criminal investigations.

I. Background

Recent news stories, along with a report released by the Department of Justice’s Office of the Inspector General (“OIG”), indicate that the government has used classified government hacking tools developed for national-security purposes in domestic criminal cases.² “Government hacking” refers to the use of malicious software (also known as “malware”) and other techniques by law enforcement agents to remotely break into and search electronic devices, and it poses significant threats to internet security, privacy, and due process rights. These threats are only compounded when the government uses classified tools developed for military and foreign espionage purposes to engage in hacking for law enforcement purposes.

Government hacking threatens the integrity of the internet. Government hacking involves collecting and exploiting flaws in widely used software and hardware — instead of reporting them so they can be patched. This risks leaving the public at the mercy of criminals and other abusers who may use the same flaw to steal data and conduct illegal surveillance. It also involves deploying hacking tools that can be stolen or misused by criminals and other governments. Additionally, the desire to hack into private devices has [motivated the U.S. government to push for widespread adoption of a flawed algorithm](#) that undermines encryption systems used by millions of people around the world.

This kind of activity runs directly counter to the government’s missions of public service and safety, and risks serious harm to third parties.³ Given that

members to lobby their legislators. The American Civil Liberties Union is a separate non-profit, 26 U.S.C. § 501(c)(4) membership organization that educates the public about the civil liberties implications of pending and proposed state and federal legislation, provides analysis of pending and proposed legislation, directly lobbies legislators, and mobilizes its members to lobby their legislators.

² Joseph Cox, *The FBI Used Classified Hacking Tools in Ordinary Criminal Investigations*, Motherboard (Mar. 29, 2018), https://motherboard.vice.com/en_us/article/7xdxg9/fbi-hacking-investigations-classified-remote-operations-unit; U.S. Dep’t of Justice, Office of the Inspector General, *A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation* 4 (2018), <https://oig.justice.gov/reports/2018/o1803.pdf>.

³ See Ellen Nakashima, *Russian military was behind ‘NotPetya’ cyberattack in Ukraine, CIA concludes*, Wash. Post (Jan. 12, 2018), <https://wapo.st/2rHHyQB>.

many of our daily activities are conducted in the digital world, we should expect government agents to improve security rather than exploit existing weaknesses or create new ones.

In addition, government hacking—which can give the government unauthorized access to private electronic devices, including mobile phones, laptops, and personal computers—raises serious privacy concerns. In *Riley v. California*, the Supreme Court made clear that individuals’ collection of digital information constitute the “privacies of life,” which include “the intimate and private details of a person’s day: from family budgets, to conversations with a partner, to love letters, to evening prayers.”⁴ Taken together and across time, these details comprise a comprehensive portrait of a person’s political preferences, religious practices, and associations. Government hacking of electronic devices like laptops, cell phones, and tablets, is an extreme invasion of one of the most private spaces an individual has.

Moreover, not only can government hacking give government actors access to an unprecedented amount of sensitive information, but the technique can be used to spread malware to large groups of people without any individualized or particular justification. In recent years, the FBI has employed the so-called “watering hole” tactic in several criminal investigations to infect all visitors to a particular website or set of websites—including, in at least one largescale FBI investigation, sites that hosted an email service used by dissidents and journalists.⁵ This tactic and others like it threaten to subvert constitutional protections from unwarranted and unreasonable government searches and seizures of private spaces and information.

The deployment of classified malware exacerbates these constitutional concerns by compromising the due process rights of individuals whose devices are searched. When the government uses classified hacking tools for law enforcement purposes, the security and privacy concerns discussed above are compounded because the judicial process may be severely hamstrung by the need for heightened secrecy. This threatens to violate defendants’ rights to a fair and public trial, and the public’s right of access to information about criminal proceedings.

In March 2018, the Oversight and Review Division of the U.S. Department of Justice’s OIG released a report titled, “A Special Inquiry

⁴ 134 S. Ct. 2473, 2495 (2014).

⁵ Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, *Wired* (Sept. 13, 2013), <https://www.wired.com/2013/09/freedom-hosting-fbi>; Ellen Nakashima, *This is how the government is catching people who use child porn sites*, *Wash. Post* (Jan. 21, 2016), http://wpo.st/_IRh1; see ACLU, *Challenging Government Hacking in Criminal Cases* (March 2017), https://www.aclu.org/sites/default/files/field_document/malware_guide_3-30-17-v2.pdf.

Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation.” The report details the examination of the FBI’s technical efforts to hack the encrypted mobile phone of the 2015 San Bernardino mass shooter, Syed Rizwan Farook.⁶ It reveals that, on February 11, 2015, the Chief of an FBI unit called the Remote Operations Unit (“ROU”) started looking into the case.⁷ The chief of the ROU explained that at the time, it was his understanding that the ROU’s classified national-security hacking tools had not been used in domestic criminal cases up until that point in early 2015.⁸ That understanding informed his determination that the application of national-security hacking tools to domestic cases was a “line in the sand” that, according to Department policy, was only to be crossed with personal approval of the Deputy Attorney General.⁹ Footnote 3 of the report suggests that the referenced policy is a January 2002 policy announced by then–Deputy Attorney General Larry Thompson entitled “Procedures for the Use of Classified Investigative Technologies in Criminal Cases.”¹⁰ Ultimately, however, the ROU contacted an outside vendor who finished developing a technique that criminal investigators used to access data on Farook’s iPhone.

The March 2018 OIG Report reveals that, since the institution of this policy in 2002, there have been at least two instances in which the Deputy Attorney General authorized the use of classified tools in a criminal case.

Notwithstanding the weight of the interests involved, little is publicly known about the government’s use of classified hacking tools domestically. Left unchecked, the government’s deployment of classified hacking tools in domestic cases seriously threatens our constitutional rights to due process and to be free from unreasonable searches and seizures. The ACLU submits this FOIA Request to provide the public with much-needed information about this privacy-invasive and potentially destructive government technique.

II. Requested Records

⁶ Lorenzo Franceschi-Bicchierai, *FBI Barely Tried to Hack San Bernardino iPhone Before Going to Court With Apple*, Motherboard (Mar. 27, 2018), https://motherboard.vice.com/en_us/article/qvxkz7/fbi-apple-san-bernardino-iphone-doj-oig-report.

⁷ U.S. Dept. of Justice, Office of the Inspector General, *A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation* 4 (2018), <https://oig.justice.gov/reports/2018/o1803.pdf>.

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.*

- (1) The Department of Justice policy requiring approval from the Deputy Attorney General for the government to use classified hacking techniques in criminal cases, as described in footnote 3 of the March 2018 report from the Department of Justice’s OIG titled, “A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation.”
- (2) The document authored by then–Deputy Attorney General Larry D. Thompson titled “Memorandum to the Assistant Attorney General of the Criminal Division, et al., Procedures for the Use of Classified Investigative Technologies in Criminal Cases” and dated January 31, 2002.
- (3) Records concerning the DOJ’s invocation of, discussion of, reliance on, or reference to the policy requiring the Deputy Attorney General’s approval for the government’s use of classified hacking tools in criminal investigations or cases, including the two cases referenced by ROU Chief in footnote 3 of the March 2018 OIG report; and
- (4) All motions, legal briefs, applications, responses, objections, court orders, court opinions, or other legal filings related to any use of classified hacking tools in criminal investigations or cases.

With respect to the form of production, *see* 5 U.S.C. § 552(a)(3)(B), the ACLU requests that responsive electronic records be provided electronically in their native file format, if possible. Alternatively, the ACLU requests that the records be provided electronically in a text-searchable, static-image format (PDF), in the best image quality in the agency’s possession, and that the records be provided in separate, Bates-stamped files.

III. Application for Expedited Processing

The ACLU requests expedited processing pursuant to 5 U.S.C. § 552(a)(6)(E).¹¹ There is a “compelling need” for these records, as defined in the statute, because the information requested is “urgen[tly]” needed by an organization primarily engaged in disseminating information “to inform the public concerning actual or alleged Federal Government activity.” 5 U.S.C. § 552(a)(6)(E)(v)(II).

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

¹¹ *See also* 28 C.F.R. § 16.5(e).

The ACLU is “primarily engaged in disseminating information” within the meaning of the statute. 5 U.S.C. § 552(a)(6)(E)(v)(II).¹² Obtaining information about government activity, analyzing that information, and widely publishing and disseminating that information to the press and public are critical and substantial components of the ACLU’s work and are among its primary activities. *See ACLU v. DOJ*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004) (finding 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” to be “primarily engaged in disseminating information”).¹³

The ACLU regularly publishes *STAND*, a print magazine that reports on and analyzes civil liberties-related current events. The magazine is disseminated to over 980,000 people. The ACLU also publishes regular updates and alerts via email to over 3.1 million subscribers (both ACLU members and non-members). These updates are additionally broadcast to over 3.8 million social media followers. The magazine as well as the email and social-media alerts often include descriptions and analysis of information obtained through FOIA requests.

The ACLU also regularly issues press releases to call attention to documents obtained through FOIA requests, as well as other breaking news,¹⁴ and ACLU attorneys are interviewed frequently for news stories about documents released through ACLU FOIA requests.¹⁵

¹² *See also* 28 C.F.R. § 16.5(e)(1)(ii).

¹³ Courts have found that the ACLU as well as other organizations with similar missions that engage in information-dissemination activities similar to the ACLU are “primarily engaged in disseminating information.” *See, e.g., Leadership Conference on Civil Rights v. Gonzales*, 404 F. Supp. 2d 246, 260 (D.D.C. 2005); *ACLU*, 321 F. Supp. 2d at 29 n.5; *Elec. Privacy Info. Ctr. v. DOD*, 241 F. Supp. 2d 5, 11 (D.D.C. 2003).

¹⁴ *See, e.g.,* Press Release, American Civil Liberties Union, U.S. Releases Drone Strike ‘Playbook’ in Response to ACLU Lawsuit (Aug. 6, 2016), <https://www.aclu.org/news/us-releases-drone-strike-playbook-response-aclu-lawsuit>; Press Release, American Civil Liberties Union, Secret Documents Describe Graphic Abuse and Admit Mistakes (June 14, 2016), <https://www.aclu.org/news/cia-releases-dozens-torture-documents-response-aclu-lawsuit>; Press Release, American Civil Liberties Union, U.S. Releases Targeted Killing Memo in Response to Long-Running ACLU Lawsuit (June 23, 2014), <https://www.aclu.org/national-security/us-releases-targeted-killing-memo-response-long-running-aclu-lawsuit>; Press Release, American Civil Liberties Union, Justice Department White Paper Details Rationale for Targeted Killing of Americans (Feb. 4, 2013), <https://www.aclu.org/national-security/justice-department-white-paper-details-rationale-targeted-killing-americans>; Press Release, American Civil Liberties Union, Documents Show FBI Monitored Bay Area Occupy Movement (Sept. 14, 2012), <https://www.aclu.org/news/documents-show-fbi-monitored-bay-area-occupy-movement-insidebayareacom>.

¹⁵ *See, e.g.,* Cora Currier, *TSA’s Own Files Show Doubtful Science Behind Its Behavioral Screen Program*, Intercept, Feb. 8, 2017, <https://theintercept.com/2017/02/08/tsas-own-files->

Similarly, the ACLU publishes reports about government conduct and civil liberties issues based on its analysis of information derived from various sources, including information obtained from the government through FOIA requests. This material is broadly circulated to the public and widely available to everyone for no cost or, sometimes, for a small fee. ACLU national projects regularly publish and disseminate reports that include a description and analysis of government documents obtained through FOIA requests.¹⁶ The ACLU also regularly publishes books, “know your rights” materials, fact sheets, and educational brochures and pamphlets designed to educate the public about civil liberties issues and government policies that implicate civil rights and liberties.

The ACLU publishes a widely read blog where original editorial content reporting on and analyzing civil rights and civil liberties news is posted daily. See <https://www.aclu.org/blog>. The ACLU creates and disseminates original editorial and educational content on civil rights and civil liberties news through multi-media projects, including videos, podcasts, and interactive features. See <https://www.aclu.org/multimedia>. The ACLU also publishes, analyzes, and disseminates information through its heavily visited website, www.aclu.org. The website addresses civil rights and civil liberties issues in depth, provides features on civil rights and civil liberties issues in the news, and contains many

show-doubtful-science-behind-its-behavior-screening-program/ (quoting ACLU attorney Hugh Handeyside); Karen DeYoung, *Newly Declassified Document Sheds Light on How President Approves Drone Strikes*, Wash. Post, Aug. 6, 2016, <http://wapo.st/2jy62cW> (quoting former ACLU deputy legal director Jameel Jaffer); Catherine Thorbecke, *What Newly Released CIA Documents Reveal About ‘Torture’ in Its Former Detention Program*, ABC, June 15, 2016, <http://abcn.ws/2jy40d3> (quoting ACLU staff attorney Dror Ladin); Nicky Woolf, *US Marshals Spent \$10M on Equipment for Warrantless Stingray Device*, Guardian, Mar. 17, 2016, <https://www.theguardian.com/world/2016/mar/17/us-marshals-stingray-surveillance-airborne> (quoting ACLU attorney Nate Wessler); David Welna, *Government Suspected of Wanting CIA Torture Report to Remain Secret*, NPR, Dec. 9, 2015, <http://n.pr/2jy2p71> (quoting ACLU project director Hina Shamsi).

¹⁶ See, e.g., Hugh Handeyside, *New Documents Show This TSA Program Blamed for Profiling Is Unscientific and Unreliable — But Still It Continues* (Feb. 8, 2017, 11:45 AM), <https://www.aclu.org/blog/speak-freely/new-documents-show-tsa-program-blamed-profiling-unscientific-and-unreliable-still>; Carl Takei, *ACLU-Obtained Emails Prove that the Federal Bureau of Prisons Covered Up Its Visit to the CIA’s Torture Site* (Nov. 22, 2016, 3:15 PM), <https://www.aclu.org/blog/speak-freely/aclu-obtained-emails-prove-federal-bureau-prisons-covered-its-visit-cias-torture>; Brett Max Kaufman, *Details Abound in Drone ‘Playbook’ – Except for the Ones That Really Matter Most* (Aug. 8, 2016, 5:30 PM), <https://www.aclu.org/blog/speak-freely/details-abound-drone-playbook-except-ones-really-matter-most>; Nathan Freed Wessler, *ACLU- Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida* (Feb. 22, 2015, 5:30 PM), <https://www.aclu.org/blog/free-future/aclu-obtained-documents-reveal-breadth-secretive-stingray-use-florida>; Ashley Gorski, *New NSA Documents Shine More Light into Black Box of Executive Order 12333* (Oct. 30, 2014, 3:29 PM), <https://www.aclu.org/blog/new-nsa-documents-shine-more-light-black-box-executive-order-12333>; ACLU, *ACLU Eye on the FBI: Documents Reveal Lack of Privacy Safeguards and Guidance in Government’s “Suspicious Activity Report” Systems* (Oct. 29, 2013), https://www.aclu.org/sites/default/files/assets/eye_on_fbi_-_sars.pdf.

thousands of documents relating to the issues on which the ACLU is focused. The ACLU's website also serves as a clearinghouse for news about ACLU cases, as well as analysis about case developments, and an archive of case-related documents. Through these pages, and with respect to each specific civil liberties issue, the ACLU provides the public with educational material, recent news, analyses of relevant Congressional or executive branch action, government documents obtained through FOIA requests, and further in-depth analytic and educational multi-media features.

The ACLU website includes many features on information obtained through the FOIA.¹⁷ For example, the ACLU's "Predator Drones FOIA" webpage, <https://www.aclu.org/national-security/predator-drones-foia>, contains commentary about the ACLU's FOIA request, press releases, analysis of the FOIA documents, numerous blog posts on the issue, documents related to litigation over the FOIA request, frequently asked questions about targeted killing, and links to the documents themselves. Similarly, the ACLU maintains an online "Torture Database," a compilation of over 100,000 pages of FOIA documents that allows researchers and the public to conduct sophisticated searches of FOIA documents relating to government policies on rendition, detention, and interrogation.¹⁸

The ACLU has also published a number of charts and explanatory materials that collect, summarize, and analyze information it has obtained through the FOIA. For example, through compilation and analysis of information gathered from various sources—including information obtained from the government through FOIA requests—the ACLU created an original chart that provides the public and news media with a comprehensive summary

¹⁷ See, e.g., Nathan Freed Wessler & Dyan Cortez, *FBI Releases Details of 'Zero-Day' Exploit Decisionmaking Process* (June 26, 2015, 11:00 AM), <https://www.aclu.org/blog/free-future/fbi-releases-details-zero-day-exploit-decisionmaking-process>; Nathan Freed Wessler, *FBI Documents Reveal New Information on Baltimore Surveillance Flights* (Oct. 30, 2015, 8:00 AM), <https://www.aclu.org/blog/free-future/fbi-documents-reveal-new-information-baltimore-surveillance-flights>; *ACLU v. DOJ – FOIA Case for Records Relating to the Killing of Three U.S. Citizens*, ACLU Case Page, <https://www.aclu.org/national-security/anwar-al-awlaki-foia-request>; *ACLU v. Department of Defense*, ACLU Case Page, <https://www.aclu.org/cases/aclu-v-department-defense>; *Mapping the FBI: Uncovering Abusive Surveillance and Racial Profiling*, ACLU Case Page, <https://www.aclu.org/mappingthefbi>; *Bagram FOIA*, ACLU Case Page <https://www.aclu.org/cases/bagram-foia>; *CSRT FOIA*, ACLU Case Page, <https://www.aclu.org/national-security/csrt-foia>; *ACLU v. DOJ – Lawsuit to Enforce NSA Warrantless Surveillance FOIA Request*, ACLU Case Page, <https://www.aclu.org/aclu-v-doj-lawsuit-enforce-nsa-warrantless-surveillance-foia-request>; *Patriot FOIA*, ACLU Case Page, <https://www.aclu.org/patriot-foia>; *NSL Documents Released by DOD*, ACLU Case Page, <https://www.aclu.org/nsl-documents-released-dod?redirect=credirect/32088>.

¹⁸ *The Torture Database*, ACLU, <https://www.thetorturedatabase.org>; see also *Countering Violent Extremism FOIA Database*, ACLU, <https://www.aclu.org/foia-collection/cve-foia-documents>; *TSA Behavior Detection FOIA Database*, ACLU, <https://www.aclu.org/foia-collection/tsa-behavior-detection-foia-database>; *Targeted Killing FOIA Database*, ACLU, <https://www.aclu.org/foia-collection/targeted-killing-foia-database>.

index of Bush-era Office of Legal Counsel memos relating to interrogation, detention, rendition, and surveillance.¹⁹ Similarly, the ACLU produced an analysis of documents released in response to a FOIA request about the TSA's behavior detection program²⁰; a summary of documents released in response to a FOIA request related to the FISA Amendments Act²¹; a chart of original statistics about the Defense Department's use of National Security Letters based on its own analysis of records obtained through FOIA requests²²; and an analysis of documents obtained through FOIA requests about FBI surveillance flights over Baltimore.²³

The ACLU plans to analyze, publish, and disseminate to the public the information gathered through this Request. The records requested are not sought for commercial use and the requesters plan 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. *See* 5 U.S.C. § 552(a)(6)(E)(v)(II).²⁴ Specifically, the requested records relate the involvement of the FBI's ROU using classified hacking tools in criminal investigations. As discussed in Part I, *supra*, the government's use of classified hacking tools in criminal investigations is the subject of widespread public controversy and media attention.²⁵

* * *

Given the foregoing, the ACLU has satisfied the requirements for expedited processing of this Request.

¹⁹ *Index of Bush-Era OLC Memoranda Relating to Interrogation, Detention, Rendition and/or Surveillance*, ACLU (Mar. 5, 2009), https://www.aclu.org/sites/default/files/pdfs/safefree/olcmemos_2009_0305.pdf.

²⁰ *Bad Trip: Debunking the TSA's 'Behavior Detection' Program*, ACLU (2017), https://www.aclu.org/sites/default/files/field_document/dem17-tsa_detection_report-v02.pdf.

²¹ *Summary of FISA Amendments Act FOIA Documents Released on November 29, 2010*, ACLU, <https://www.aclu.org/files/pdfs/natsec/faafoia20101129/20101129Summary.pdf>.

²² *Statistics on NSL's Produced by Department of Defense*, ACLU, <https://www.aclu.org/other/statistics-nsls-produced-dod>.

²³ Nathan Freed Wessler, *FBI Documents Reveal New Information on Baltimore Surveillance Flights* (Oct. 30, 2015, 8:00 AM), <https://www.aclu.org/blog/free-future/fbi-documents-reveal-new-information-baltimore-surveillance-flights>.

²⁴ *See also* 28 C.F.R. § 16.5(e)(1)(ii).

²⁵ *See supra* notes 2, 3, & 6.

IV. Application for Waiver or Limitation of Fees

The ACLU requests a waiver of document search, review, and duplication fees on the grounds that disclosure of the requested records is in the public interest and because disclosure 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.” 5 U.S.C. § 552(a)(4)(A)(iii).²⁶ The ACLU also requests a waiver of search fees on the grounds that the ACLU qualifies as a “representative of the news media” and the records are not sought for commercial use. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

A. *The Request 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 ACLU.*

As discussed above, credible media and other investigative accounts underscore the substantial public interest in the records sought through this Request. Given the ongoing and widespread media attention to this issue, the records sought will significantly contribute to public understanding of an issue of profound public importance. Because little specific information about the government’s use of classified hacking tools is publicly available, the records sought are certain to contribute significantly to the public’s understanding of when the government uses these tools in criminal investigations.

The ACLU is not filing this Request to further its commercial interest. As described above, any information disclosed by the ACLU as a result of this FOIA Request will be available to the public at no cost. Thus, a fee waiver would fulfill Congress’s legislative intent in amending FOIA. *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.” (Quotation marks omitted)).

B. *The ACLU is a representative of the news media and the records are not sought for commercial use.*

The ACLU also requests a waiver of search fees on the grounds that the ACLU qualifies as a “representative of the news media” and the records are not sought for commercial use. 5 U.S.C. § 552(a)(4)(A)(ii)(II).²⁷ The ACLU meets the statutory and regulatory definitions 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.” 5 U.S.C.

²⁶ *See also* 28 C.F.R. § 16.10(k)(2).

²⁷ *See also* 28 C.F.R. § 16.10(k)(2)(ii)–(iii).

§ 552(a)(4)(A)(ii)(III);²⁸ *see also Nat'l Sec. Archive v. DOD*, 880 F.2d 1381, 1387 (D.C. Cir. 1989) (finding that an organization that gathers information, exercises editorial discretion in selecting and organizing documents, “devises indices and finding aids,” and “distributes the resulting work to the public” is a “representative of the news media” for purposes of the FOIA); *Serv. Women's Action Network v. DOD*, 888 F. Supp. 2d 282 (D. Conn. 2012) (requesters, including ACLU, were representatives of the news media and thus qualified for fee waivers for FOIA requests to the Department of Defense and Department of Veterans Affairs); *ACLU of Wash. v. DOJ*, No. C09-0642RSL, 2011 WL 887731, at *10 (W.D. Wash. Mar. 10, 2011) (finding that the ACLU of Washington 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”); *ACLU*, 321 F. Supp. 2d at 30 n.5 (finding non-profit public interest group to be “primarily engaged in disseminating information”). The ACLU is therefore a “representative of the news media” for the same reasons it is “primarily engaged in the dissemination of information.”

Furthermore, courts have found other organizations whose mission, function, publishing, and public education activities are similar in kind to the ACLU's to be “representatives of the news media” as well. *See, e.g., Cause of Action v. IRS*, 125 F. Supp. 3d 145 (D.C. Cir. 2015); *Elec. Privacy Info. Ctr.*, 241 F. Supp. 2d at 10–15 (finding non-profit public interest group that disseminated an electronic newsletter and published books was a “representative of the news media” for purposes of the FOIA); *Nat'l Sec. Archive*, 880 F.2d at 1387; *Judicial Watch, Inc. v. DOJ*, 133 F. Supp. 2d 52, 53–54 (D.D.C. 2000) (finding Judicial Watch, self-described as a “public interest law firm,” a news media requester).²⁹

On account of these factors, fees associated with responding to FOIA requests are regularly waived for the ACLU as a “representative of the news media.”³⁰ As was true in those instances, the ACLU meets the requirements for a fee waiver here.

²⁸ *See also* 28 C.F.R. § 16.10(b)(6).

²⁹ Courts have found these organizations to be “representatives of the news media” even though they engage in litigation and lobbying activities beyond their dissemination of information / public education activities. *See, e.g., Elec. Privacy Info. Ctr.*, 241 F. Supp. 2d 5; *Nat'l Sec. Archive*, 880 F.2d at 1387; *see also Leadership Conference on Civil Rights*, 404 F. Supp. 2d at 260; *Judicial Watch, Inc.*, 133 F. Supp. 2d at 53–54.

³⁰ In May 2016, the FBI granted a fee-waiver request regarding a FOIA request issued to the DOJ for documents related to Countering Violent Extremism Programs. In April 2013, the National Security Division of the DOJ granted a fee-waiver request with respect to a request for documents relating to the FISA Amendments Act. Also in April 2013, the DOJ granted a fee-waiver request regarding a FOIA request for documents related to “national security letters” issued under the Electronic Communications Privacy Act. In August 2013, the FBI granted the fee-waiver request related to the same FOIA request issued to the DOJ. In June 2011, the DOJ

* * *

Pursuant to applicable statutes and regulations, the ACLU expects a determination regarding expedited processing within 10 days. *See* 5 U.S.C. § 552(a)(6)(E)(ii); 28 C.F.R. § 16.5(e)(4).

If the Request is denied in whole or in part, the ACLU asks that you justify all deletions by reference to specific exemptions to FOIA. The ACLU expects the release of all segregable portions of otherwise exempt material. The ACLU reserves the right to appeal a decision to withhold any information or deny a waiver of fees.

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

Jennifer Stisa Granick
American Civil Liberties Union
39 Drumm Street
San Francisco, California 94111
T: 415.343.0758
F: 415.395.0950
jgranick@aclu.org

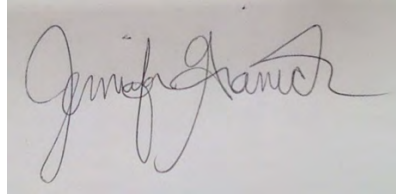
Brett Max Kaufman
American Civil Liberties Union
125 Broad Street—18th Floor
New York, New York 10004
T: 212.549.2603
F: 212.549.2654

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

National Security Division 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.

I affirm that the information provided supporting the request for expedited processing is true and correct to the best of my knowledge and belief. *See* 5 U.S.C. § 552(a)(6)(E)(vi).

Respectfully,

A rectangular image showing a handwritten signature in black ink on a light-colored background. The signature is cursive and appears to read "Jennifer Stisa Granick".

Jennifer Stisa Granick
American Civil Liberties Union
39 Drumm Street
San Francisco, California 94111
T: 415.343.0758
F: 415.395.0950
jgranick@aclu.org

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION