



August 25, 2011

Director, Freedom of Information and Security Review
Department of Defense
FOIA/Privacy Branch
1155 Defense Pentagon, Room 2C757
Washington, DC 20301-1155

Alesia Y. Williams
Chief, FOIA Services Branch
Defense Intelligence Agency
ATTN: DIAC, DAN-1A (FOIA)
200 MacDill Boulevard
Washington, DC 20340-5100

**AMERICAN CIVIL LIBERTIES
UNION FOUNDATION**
LEGAL DEPARTMENT
NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
F/212.549.2651
WWW.ACLU.ORG

David M. Hardy, Chief
Record/Information Dissemination Section, Records Management Division
Federal Bureau of Investigation
170 Marcel Drive
Winchester, VA 22602-4843

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

RICHARD ZACKS
TREASURER

Department of Justice
FOIA/PA Mail Referral Unit
LOC Building
Room 115
Justice Management Division
Washington, DC 20530-0001

Carmen L. Mallon
Chief of Staff
Office of Information Policy
Department of Justice
Suite 11050
1425 New York Avenue, NW
Washington, DC 20530-0001

Tracy Schmalzer, Acting Director
Office of Public Affairs
Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Central Intelligence Agency
FOIA Office
Gate 5
1000 Colonial Farm Road
McLean, VA 22101

Michele Smith
FOIA Contact, FOIA Requester Service Center/DJP4
National Security Agency
Suite 6248
9800 Savage Road
Fort George G. Meade, MD 20755-6248

Office of the Director of National Intelligence (ODNI)
Washington, D.C. 20511

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

Delores Barber
Deputy Chief FOIA Officer, Director, Disclosure & FOIA
The Privacy Office
U.S. Department of Homeland Security
245 Murray Drive SW, Building 410
STOP-0655
Washington, DC 20528-0655

Catrina Pavlick-Keenan
FOIA Officer
U.S. Immigration & Customs Enforcement
5th Floor, Suite 585
800 North Capital Street, NW
Washington, DC 20536-5009

Federal Communications Commission
445 12th Street, S.W., Room 1-A836
Washington, D.C. 20554

Brenda Dolan
Departmental Freedom of Information Officer
Office of Privacy and Open Government
Department of Commerce
14th and Constitution Avenue N.W.
Mail Stop H6204
Washington, DC 20230

**Re: REQUEST UNDER FREEDOM OF INFORMATION ACT
EXPEDITED PROCESSING REQUESTED**

Dear FOIA Officer,

This letter constitutes a request (“Request”) pursuant to the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552; the Department of Defense implementing regulations, 32 C.F.R. § 286.1, *et seq.*; the Department of Justice (“DOJ”) implementing regulations, 28 C.F.R. § 16.1, *et seq.*; the Central Intelligence Agency implementing regulations, 32 C.F.R. § 1900.01, *et seq.*; the Office of the Director of National Intelligence implementing regulations, 32 C.F.R. § 1700.1 *et seq.*; the Department of Homeland Security implementing regulations, 6 C.F.R. § 5.1, *et seq.*; the Federal Communications Commission implementing regulations, 47 C.F.R. § 0.461, *et seq.*; and the Department of Commerce implementing regulations, 15 C.F.R. § 4.1, *et seq.*, seeking records relating to government collection and use of information under statutes relating to cybersecurity. This Request is submitted on behalf of the American Civil Liberties Union and the American Civil Liberties Union Foundation (together, the “ACLU”).¹

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

Records Requested

The ACLU seeks records relating to requests for and disclosures of customer or user records, personal information or personally identifiable information (“PII”)², contents of electronic communications³, and malware

¹ The American Civil Liberties Union is a 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. The American Civil Liberties Union Foundation is a separate 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, and educates the public about the civil liberties implications of pending and proposed state and federal legislation, provides analyses of pending and proposed legislation, directly lobbies legislators, and mobilizes its members to lobby their legislators.

² Personal information and personally identifiable information, both referred to as “PII” and used interchangeably in this Request, shall include: name, such as full name, maiden name, mother’s maiden name, or alias; personal identification number, such as social security number, passport number, driver’s license number, taxpayer identification number, patient identification number, and financial account or credit card number; address information, such as street address or email address; asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people; telephone numbers, including mobile, business, and personal numbers; personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry); information identifying personally owned property, such as vehicle registration number or title number and related information; information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information. Nat’l Institute of Standards and Technology, U.S. Dep’t. of Commerce, NIST 800-122, Guide to Protecting the

signatures, virus signatures, heuristic signatures, or any other type of cybersecurity-related signatures, by communications providers⁴ to the federal government, for cybersecurity purposes, including but not limited to:

1. Any and all memoranda (including Office of Legal Counsel memoranda), legal interpretations, procedures, privacy impact assessments, policies, directives, practices, guidance, rules or guidelines created since January 19, 2001 relating to the request for, receipt, screening, retention or dissemination of cybersecurity-related disclosures⁵ received from communications providers.
2. Any and all inter or intra-agency correspondence created since January 19, 2001 relating to: the request for, receipt, screening, retention or dissemination of cybersecurity-related disclosures received from communications providers; legal interpretations of any law permitting the receipt, screening, retention, or dissemination of such disclosures; or procedures, privacy impact assessments,

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

Confidentiality of Personally Identifiable Information (Apr. 2010), <http://1.usa.gov/aU94uy>. It shall also include device identifiers and serial numbers, web universal resource locators (URLs), and any other unique identifying numbers, characteristics, or codes.

³ Electronic communication is defined as:

any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

- (A) any wire or oral communication;
- (B) any communication made through a tone-only paging device;
- (C) any communication from a tracking device (as defined in section 3117 of this title); or
- (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

18 U.S.C. § 2510(12).

⁴ Communications providers include public and private companies in the telecommunications, internet, cable, satellite and managed service businesses, including application service providers, network service providers, internet service providers, managed service providers, master managed service providers, managed Internet service providers, telecommunications service providers (wireless and landline), and Security Assertion Markup Language (“SAML”) service providers.

⁵ For purposes of this Request, cybersecurity-related disclosures refer to a communications provider’s disclosure or transfer to the government for cybersecurity-related purposes of customer or user records, personal information or personally identifiable information, contents of electronic communications, and malware signatures, virus signatures, heuristic signatures, or any other type of cybersecurity-related signatures, or any other information pursuant to 18 U.S.C. § 2702(b)(5), (b)(8), (c)(3) and (c)(4); 18 U.S.C. § 2511(2)(a)(i) and (2)(i); or any other cybersecurity-related statute or regulation.

policies, directives, practices, guidance, rules or guidelines governing the receipt, screening, retention, or dissemination of such disclosures.

3. Any and all correspondence created since January 19, 2001 with state and local government agencies relating to: the request for, receipt, screening, retention or dissemination of cybersecurity-related disclosures received from communications providers; legal interpretations of any law permitting the receipt, screening, retention or dissemination of such disclosures; or procedures, privacy impact assessments, policies, directives, practices, guidance, rules or guidelines governing the receipt, screening, retention or dissemination of such disclosures.
4. Any and all records created since January 19, 2001 indicating the number of:
 - a. government requests to communications providers for cybersecurity-related disclosures under the self-defense provisions of the Wiretap Act and the Electronic Communications Privacy Act, 18 U.S.C. § 2511(2)(a)(i) and 18 U.S.C. § 2702(b)(5) and 2702(c)(3), and the mechanism by which the disclosures were requested, such as, but not limited to, warrants, subpoenas, national security letters, exigent letters, other written requests, and oral requests;
 - b. cybersecurity-related disclosures by communications providers under the self-defense provisions of the Wiretap Act and the Electronic Communications Privacy Act, 18 U.S.C. § 2511(2)(a)(i) and 18 U.S.C. § 2702(b)(5) and 2702(c)(3);
 - c. government requests to communications providers for cybersecurity-related disclosures under laws relating to computer trespassers, including 18 U.S.C. § 2511(2)(i) and the mechanism by which the disclosures were requested, such as, but not limited to, warrants, subpoenas, national security letters, exigent letters, other written requests, and oral requests;
 - d. cybersecurity-related disclosures by communications providers under laws relating to computer trespassers, including 18 U.S.C. § 2511(2)(i);
 - e. government requests to communications providers for cybersecurity-related disclosures based on “emergencies involving danger of death or serious physical injury to any person,” 18 USC § 2702(b)(8) and 2702(c)(4), and the mechanism by which the disclosures were requested, such as, but not limited to, warrants, subpoenas, national security letters, exigent letters, other written requests, and oral requests;

- f. cybersecurity-related disclosures by communications providers based on “emergencies involving danger of death or serious physical injury to any person,” 18 USC § 2702(b)(8) and 2702(c)(4);
 - g. government requests to communications providers for cybersecurity-related disclosures under the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801, *et seq.*;
 - h. cybersecurity-related disclosures by communications providers under the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801, *et seq.*;
 - i. government requests to communications providers for malware signatures, virus signatures, heuristic signatures, or any other type of cybersecurity-related signatures, and the legal authority for the requests;
 - j. disclosures of malware signatures, virus signatures, heuristic signatures, or any other type of cybersecurity-related signatures, by communications providers and the legal authority for the disclosures;
 - k. any other governmental requests to communications providers for cybersecurity-related disclosures, the legal justification for the requests, and the mechanism by which the disclosures were requested, such as, but not limited to, warrants, subpoenas, national security letters, exigent letters, other written requests, and oral requests; and
 - l. any other cybersecurity-related disclosures by communications providers and the legal justification for the disclosures.
5. For all items in Request #4 above, any and all records created since January 19, 2001 indicating:
- a. the number of times communications providers voluntarily made disclosures to the government without a request and the legal justification for such disclosures;
 - b. the number of individuals, corporations, non-profits and other entities, including labor unions and activist groups, about whom disclosures were requested;
 - c. the number of requests from the government for cybersecurity-related disclosures with which communications providers complied in full;
 - d. the number of requests from the government for cybersecurity-related disclosures with which communications providers refused to comply in whole or in part, and the reasons for those refusals, including any discussion of the First Amendment to the Constitution and any information relating to the type of entity about which information was sought (including individual, corporation, non-profit, labor union, activist group, etc.);

- e. the number of instances in which after communications providers refused to comply in whole or in part with government requests for cybersecurity-related disclosures, the government: a) sought court orders for the disclosures and the result of those court proceedings; or b) issued subpoenas or other mechanisms for the disclosures, including any information relating to the type of entity about which information was sought (including individual, corporation, non-profit, labor union, activist group, etc.);
 - f. the number of times communications providers went to court to quash subpoenas for cybersecurity-related disclosures or to challenge other mechanisms requesting or requiring cybersecurity-related disclosures, and the outcome of those proceedings, including any information relating to the type of entity about which information was sought (including individual, corporation, non-profit, labor union, activist group, etc.);
 - g. the number of requests for cybersecurity-related disclosures the government initiated then dropped before receiving such disclosures, and the number of such request with which the communications providers refused to comply in whole or in part before the request was dropped, including any information relating to the type of entity about which information was sought (including individual, corporation, non-profit, labor union, activist group, etc.);
 - h. the number of times communications providers informed the government they had no relevant disclosures to provide;
 - i. the number of prosecutions, deportation proceedings, or other law enforcement proceedings that resulted from cybersecurity-related disclosures or requests for such disclosures;
 - j. the number of times communications providers provided disclosures beyond those requested by the government and the government's response to that action; and
 - k. the number of times communications providers provided disclosures beyond that permitted under existing legal authority and the government's response to that action.
6. Any and all documents created since January 19, 2001 indicating whether the cybersecurity-related disclosures sought by the government or provided by the communications providers were for information provided prospectively, in real time, or based on historical records or data, and if historical, the age of the information sought.
7. Any and all documents created since January 19, 2001 indicating what was done with cybersecurity-related disclosures received from communications providers, including how long the disclosures were kept by the receiving agency; whether any disclosures were

disseminated, and if so, to whom and for what purpose; and whether any of the disclosures were destroyed and if so, how long they were retained before they were destroyed, including any information relating to whether the disclosures were provided at the request of the government.

8. Any and all reports, assessments, including privacy impact assessments, or reviews issued or conducted, relating to the request for, receipt and screening of, and retention and dissemination of cybersecurity-related disclosures received from, communications providers, created since January 19, 2001, including any such materials created by the offices of the Attorney General, Director of National Intelligence, the head of any other intelligence agency, the Director of the Federal Bureau of Investigation, the Inspector General of the Department of Justice, or the Inspector General of any other agency included in this request.
9. Any and all records created since January 19, 2001 concerning complaints about, investigations of, or disciplinary actions related to, request for cybersecurity-related disclosures from communications providers or the sharing of cybersecurity-related disclosures by communications providers with the government.
10. Any and all records created since January 19, 2001 relating to reimbursements requested or received by communications providers for expenses related to cybersecurity-related disclosures, including the legal justification for those reimbursements.

With respect to the form of production, *see* 5 U.S.C. § 552(a)(3)(B), we request that responsive electronic records be provided electronically in their native file format, if possible. Alternatively, we request 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.

Application for Expedited Processing

We request expedited processing pursuant to 5 U.S.C. § 552(a)(6)(E); 32 C.F.R. § 286.4(d)(3); 28 C.F.R. § 16.5(d); 32 C.F.R. § 1700.12; 6 C.F.R. § 5.5(d); 47 C.F.R. § 0.461(h); and 15 C.F.R. § 4.6(e). Expedited processing is warranted because the information requested is urgently needed by an organization primarily engaged in disseminating information in order to inform the public about actual or alleged federal government activity, 5 U.S.C. § 552(a)(6)(E)(v)(II); 32 C.F.R. § 286.4(d)(3)(ii); 28 C.F.R. § 16.5(d)(1)(ii); 32 C.F.R. § 1700.12(2); 6 C.F.R. § 5.5(d)(3)(ii); 47 C.F.R. § 0.461(h)(1)(ii); 15 C.F.R. § 4.6(e)(1)(iv),

and because the records sought relate to a “matter of widespread and exceptional media interest in which there exist possible questions about the government’s integrity which affect public confidence,” 28 C.F.R. § 16.5(d)(1)(iv); 15 C.F.R. § 4.6(e)(iii).

A. The requester is primarily engaged in the dissemination of information.

The ACLU is “primarily engaged in disseminating information” within the meaning of the statute and regulations. Obtaining information about government activity, analyzing that information, and publishing and widely disseminating that information to the press and public (in both its raw and analyzed form) is a critical and substantial component of the ACLU’s work and one of its primary activities. *See Am. Civil Liberties Union 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” to be “primarily engaged in disseminating information” (internal citation and quotation marks omitted)).

Although the ACLU is perhaps most well known for its litigation activities, it is far more than a large public-interest law firm. The ACLU’s principal mission is not to litigate important civil-rights and civil-liberties cases, but to preserve and defend the guarantees of the Bill of Rights and civil-rights laws, using litigation as just one of many tactics. Every aspect of the ACLU’s work in furtherance of this mission—including litigation—can fairly be described as information dissemination. Indeed, public education and dissemination of information is a key component of the ACLU’s litigation efforts; litigation is a highly effective vehicle for educating the press and public about civil-liberties problems.

Most ACLU cases have dedicated webpages through which the ACLU publishes and disseminates information about the cases themselves (*i.e.*, case developments, analyses of case developments, a comprehensive archive of court filings, and judicial opinions); these efforts, even standing alone, are a significant endeavor in publication and dissemination of news. Case webpages, however, do not just disseminate information about case developments; these webpages also have educational material about the particular civil-liberties issue or problem, recent news about the particular issue, analyses of congressional or executive-branch action on the particular issue, governmental documents obtained through FOIA about the particular issue, and more in-depth analytic and educational multimedia features on the issue. For example, the ACLU’s website about its national security letter (“NSL”) cases, <http://www.aclu.org/nsl>, includes, among other things, an explanation of what NSLs are; information about and document repositories

for the ACLU's NSL cases; links to documents obtained through FOIA about various agencies' use of NSLs; NSL news in the courts, Congress, and executive agencies; links to original blog posts commenting on and analyzing NSL-related news; educational web features about the NSL gag-order power; public education reports about NSLs and the Patriot Act; news about and analysis of the Department of Justice Inspector General's reviews of the FBI's use of NSLs; the ACLU's policy analysis and recommendations for reform of the NSL power; charts with analyzed data about the government's use of NSLs; "myths-and-facts" documents; and links to information and analysis of related issues.⁶

The ACLU publishes newsletters, news briefings, right-to-know handbooks, and other materials that are disseminated to the public. Its material is available to everyone, including tax-exempt organizations, not-for-profit groups, law students, and faculty, for no cost or for a nominal fee.

The ACLU also regularly issues press releases to call attention to documents released through FOIA and other breaking news. *See, e.g.*, Press Release, Am. Civil Liberties Union, Important Electronic Privacy Information Legislation Introduced In Senate (May 17, 2011), <http://www.aclu.org/technology-and-liberty/important-electronic-privacy-information-legislation-introduced-senate>; Press Release, Am. Civil Liberties Union, Justice Department Asks Appeals Court To Reconsider Ruling Allowing Challenge To Warrantless Wiretapping Law (May 13, 2011), <http://www.aclu.org/national-security/justice-department-asks-appeals-court-reconsider-ruling-allowing-challenge-warrant>; Press Release, Am. Civil Liberties Union, New Reports on 9/11 Interrogation Tapes Underscore Need For Full Accountability And Transparency, Says ACLU (Aug. 17, 2010), <http://www.aclu.org/national-security/new-reports-911-interrogation-tapes-underscore-need-full-accountability-and-transp>; Press Release, Am. Civil Liberties Union, ACLU Files Lawsuit Challenging Unconstitutional "No Fly List" (June 30, 2010), <http://www.aclu.org/national-security/aclu-files-lawsuit-challenging-unconstitutional-no-fly-list>; Press Release, Am. Civil Liberties Union, ACLU Calls on Administration and Congress To Follow The Rule of Law In Terrorism Cases (May 4, 2010), <http://www.aclu.org/national-security/aclu-calls-administration-and-congress-follow-rule-law-terrorism-cases>; Press Release, Am. Civil Liberties Union, Newly Released Documents Reveal Details of Civilian Casualty Claims in Afghanistan and Iraq (Apr. 1, 2010), <http://www.aclu.org/national-security/newly-released>

⁶ For a sampling of other similar case pages with case information, reporting of news on the issue, blogs, and original analytic and educational content, see: <http://www.aclu.org/lgbt/relationships/californiamarriage.html> (same-sex marriage case page); <http://www.aclu.org/safefree/rendition/index.html> (extraordinary rendition case page); <http://www.aclu.org/immigrants/detention/hutto.html> (immigration detention conditions case page).

documents-reveal-details-civilian-casualty-claims-afghanistan-and-i; Press Release, Am. Civil Liberties Union, Most Guantanamo Detainees Were Not Involved In Plots Against U.S., Report Reveals (May 29, 2010), <http://www.aclu.org/national-security/most-guantanamo-detainees-were-not-involved-plots-against-us-report-reveals>; Press Release, Am. Civil Liberties Union, ACLU Files Habeas Corpus Petitions On Behalf Of Four Bagram Detainees (Feb. 26, 2010), <http://www.aclu.org/national-security/aclu-files-habeas-corpus-petitions-behalf-four-bagram-detainees>; Press Release, Am. Civil Liberties Union, Internal Report Finds Flagrant National Security Letter Abuse By FBI (Jan. 20, 2010), <http://www.aclu.org/national-security/internal-report-finds-flagrant-national-security-letter-abuse-fbi>.

ACLU attorneys are frequently quoted in news stories about documents requested or released through ACLU FOIA requests. *See, e.g.*, Joshua E.S. Phillips, *Inside the Detainee Abuse Task Force*, *The Nation*, May 30, 2011 (quoting ACLU staff attorney Alexander Abdo); Scott Shane & Benjamin Weiser, *Dossier Shows Push for More Attacks After 9/11*, *N.Y. Times*, Apr. 25, 2011 (quoting ACLU project director Hina Shamsi); Eric Lichtblau, *Court Revives Lawsuit Over Government Surveillance*, *N.Y. Times*, Mar. 21, 2011 (quoting ACLU deputy legal director Jameel Jaffer).

The ACLU regularly publishes a newsletter at least twice a year that reports on and analyzes civil-liberties-related current events. The newsletter is distributed to approximately 450,000 people. The ACLU also publishes a bi-weekly electronic newsletter, which is distributed to subscribers (both ACLU members and non-members) by e-mail. The electronic newsletter is distributed to approximately 300,000 people. Both of these newsletters often include descriptions and analyses of information obtained from the government through FOIA, as well as information about cases, governmental policies, pending legislation, abuses of constitutional rights, and polling data. *Cf. Elec. Privacy Info. Ctr. v. Dep't of Def.*, 241 F. Supp. 2d 5, 13–14 (D.D.C. 2003) (finding EPIC to be a representative of the news media under Department of Defense regulations because it published a “bi-weekly electronic newsletter that is distributed to over 15,000 readers” about “court cases and legal challenges, government policies, legislation, civil rights, surveys and polls, legislation, privacy abuses, international issues, and trends and technological advancements”); *Ctr. for Pub. Integrity v. Dep't of Health & Human Servs.*, No. 06-1818 (JDB), 2007 WL 2248071, at *5 (D.D.C. Aug. 3, 2007) (finding CPI to be a news-media requester because its journalist members “write and post an online newsletter” and post information obtained through FOIA in that newsletter); 32 C.F.R. § 286.28(e)(7)(i) (“The term ‘representative of the news media’ refers to any person actively gathering news for an entity that is organized and operated to publish or broadcast news to the public [including] publishers of periodicals . . .”).

The ACLU regularly publishes reports about governmental activity and civil-liberties issues based on its analysis of information derived from various sources, including information obtained from the government through FOIA.⁷ This material is broadly circulated to the public and available to everyone, including individuals, tax-exempt organizations, not-for-profit groups, and law students and faculty, for no cost or for a nominal fee. See *Elec. Privacy Info. Ctr.*, 241 F. Supp. 2d at 11 (finding EPIC a news-media requester because it “researches issues on privacy and civil liberties, reports on this information, analyzes relevant data, evaluates the newsworthiness of material and puts the facts and issues into context, publishing and distributing this ‘news’ through the sale of its books to the public”); see also *Nat’l Sec. Archive v. Dep’t of Def.*, 880 F.2d 1381, 1386 (D.C. Cir. 1989) (finding National Security Archive to be a news-media requester because it intended to publish “document sets” on “topic[s] of current interest”).⁸

⁷ See, e.g., *Policing Free Speech: Police Surveillance and Obstruction of First Amendment-Protected Activity* (Aug. 2010), http://www.aclu.org/files/assets/policingfreespeech_20100806.pdf; *Establishing A New Normal: National Security, Civil Liberties, and Human Rights Under the Obama Administration* (July 2010), <http://www.aclu.org/files/assets/EstablishingNewNormal.pdf>; *Report of the American Civil Liberties Union on the Nomination of Elena Kagan to be Associate Justice of the U.S. Supreme Court* (June 2010), <http://www.aclu.org/files/assets/2010-6-21-KaganReport-SCOTUS.pdf>; *Sentenced to Stigma* (Apr. 2010), <http://www.aclu.org/files/assets/health0410webwcover.pdf>; *America Unrestored* (Jan. 2010), http://www.aclu.org/files/pages/americau unrestored_11_20100119.pdf; *Mental Illness and the Death Penalty* (May 2009), http://www.aclu.org/pdfs/capital/mental_illness_may2009.pdf; *Human Rights Begin at Home* (Apr. 2009), http://www.udhr60.org/human_rights_full.pdf; *Reclaiming Patriotism* (Mar. 2009), http://www.aclu.org/pdfs/safefree/patriot_report_20090310.pdf; *Missing the Mark: Alternative Schools in the State of Mississippi* (Feb. 2009), http://www.aclu.org/pdfs/racialjustice/missingthemark_report.pdf; *A Looming Crisis* (Dec. 2008), http://www.aclum.org/lockingupkids/pdf/looming_crisis_web.pdf; *De Facto Disenfranchisement* (Oct. 2008), http://www.aclu.org/pdfs/racialjustice/defactodisenfranchisement_report.pdf; *A Violent Education: Corporal Punishment of Children in U.S. Public Schools* (Aug. 2008), http://www.aclu.org/pdfs/humanrights/aviolenteducation_report.pdf; *Fusion Center Update* (July 2008), http://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf; *Enacting a Reasonable Federal Shield Law* (July 2008), http://www.aclu.org/images/asset_upload_file113_35870.pdf; *Locking Up Our Children* (May 2008), http://www.aclu.org/pdfs/racialjustice/locking_up_our_children_web_ma.pdf; *Pandemic Preparedness: The Need for a Public Health—Not a Law Enforcement/National Security—Approach* (Jan. 2008), http://www.aclu.org/images/asset_upload_file399_33642.pdf.

⁸ In addition to the national ACLU offices, there are 53 ACLU affiliate and national-chapter offices located throughout the United States and Puerto Rico. These offices further disseminate ACLU material to local residents, schools, and organizations through a variety of means, including their own websites, publications, and newsletters. Further, the ACLU makes archived material available at the American Civil Liberties Union Archives at the Princeton University Library.

The ACLU also regularly publishes books, “know your rights” publications, fact sheets, and educational brochures and pamphlets designed to educate the public about civil-liberties issues and governmental policies that implicate civil rights and liberties. Some of the recent books published by the ACLU include: Lenora M. Lapidus, Emily J. Martin & Namita Luthra, *The Rights of Women: The Authoritative ACLU Guide to Women’s Rights* (NYU Press 2009); Jameel Jaffer & Amrit Singh, *Administration of Torture: A Documentary Record from Washington to Abu Ghraib and Beyond* (Columbia Univ. Press 2007) (a book based on documents obtained through FOIA).⁹ Some of the more recent “know your rights” publications include: *Gender-Based Violence & Harassment: Your School, Your Rights* (May 2011), http://www.aclu.org/files/assets/genderbasedviolence_factsheet_0.pdf; *Know Your Options at the Airport* (Nov. 2010), http://www.aclu.org/files/assets/aclu_know_your_options_at_airport_nov2010.pdf; *Know Your Rights: What to Do If You’re Stopped by Police, Immigration Agents or the FBI* (June 2010), http://www.aclu.org/files/assets/bustcard_eng_20100630.pdf. Some of the more recent ACLU fact sheets include: *Military Abortion Ban in Cases of Rape and Incest (Factsheet)* (May 13, 2011), <http://www.aclu.org/reproductive-freedom/military-abortion-ban-cases-rape-and-incest-factsheet>; *The Facts About “The No Taxpayer Funding For Abortion Act”* (Apr. 2011), http://www.aclu.org/files/assets/Chris_Smith_bill-ACLU_Fact_Sheet_UPDATED-4-30-11.pdf.¹⁰ These materials are specifically designed to be educational and widely disseminated to the public. *See Elec. Privacy Info. Ctr.*, 241 F. Supp. 2d at 11 (finding EPIC to be a news-media requester because of its publication and distribution of seven books on privacy, technology, and civil liberties); *Nat’l Sec. Archive*, 880 F.2d at 1386 (finding the National Security Archive to be a news-media requester where it had previously published only one book); *see also Leadership Conference on Civil Rights v. Gonzalez*, 404 F. Supp. 2d 246, 260 (D.D.C. 2005) (finding Leadership Conference on Civil Rights to be “primarily engaged in the dissemination of information” because it “disseminate[d] information regarding civil rights and voting rights to educate the public, promote effective civil rights laws, and ensure their enforcement by the Department of Justice”).

⁹ A search of Amazon.com conducted on August 15, 2011 produced over 50 books published by the ACLU.

¹⁰ For many more ACLU fact sheets on various civil liberties topics see: http://www.aclu.org/safefree/relatedinformation_fact_sheets.html, http://www.aclu.org/lgbt/relatedinformation_fact_sheets.html, http://www.aclu.org/privacy/relatedinformation_fact_sheets.html, http://www.aclu.org/womensrights/relatedinformation_fact_sheets.html, http://www.aclu.org/reproductiverights/relatedinformation_fact_sheets.html, and http://www.aclu.org/intlhumanrights/relatedinformation_fact_sheets.html.

The ACLU operates a widely-read blog where original editorial content reporting on and analyzing civil-rights and civil-liberties news is posted daily. See <http://blog.aclu.org/>. The ACLU also creates and disseminates original editorial and educational content on civil-rights and civil-liberties news through multimedia projects, including videos, podcasts, and interactive features. See <http://www.aclu.org/multimedia/index.html>.

The ACLU also disseminates information through its website, www.aclu.org. The website addresses civil liberties issues in depth, provides features on civil liberties issues in the news, and contains hundreds of documents that relate 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, the ACLU also provides the public with educational material about the particular civil liberties issue or problem; recent news about the issue; analyses of Congressional or executive branch action on the issue; government documents obtained through FOIA about the issue; and more in-depth analytic and educational multimedia features on the issue.

The ACLU website specifically includes features on information obtained through FOIA, including: <http://www.aclu.org/torturefoia>; <http://www.aclu.org/olcmemos/>; <http://www.aclu.org/safefree/torture/csrtfoia.html>; <http://www.aclu.org/natsec/foia/search.html>; <http://www.aclu.org/safefree/nsaspying/30022res20060207.html>; <http://www.aclu.org/patriotfoia>; www.aclu.org/spyfiles; <http://www.aclu.org/safefree/nationalsecurityletters/32140res20071011.html>; <http://www.aclu.org/exclusion>. For example, the ACLU's "Torture FOIA" webpage, <http://www.aclu.org/torturefoia>, contains commentary about the ACLU's FOIA request for documents related to the treatment of detainees, press releases, analysis of the FOIA documents disclosed, and an advanced search engine permitting webpage visitors to search the documents obtained through the FOIA, and advises that the ACLU in collaboration with Columbia University Press has published a book about the documents obtained through the FOIA. Similarly, the ACLU's webpage about the Office of Legal Counsel ("OLC") torture memos it obtained through FOIA, http://www.aclu.org/safefree/general/olc_memos.html, contains commentary and analysis of the memos; an original comprehensive chart about OLC memos (see below); links to web features created by ProPublica—an independent, non-profit, investigative-journalism organization—based on information gathering, research, and analysis conducted by the ACLU; and ACLU videos created about the memos. See *Nat'l Sec. Archive*, 880 F.2d at 1386 (finding the National Security Archive to be a news-media requester because it intended to publish "document sets" whereby its staff would "cull

those of particular interest . . . supplement the chosen documents with ‘detailed cross-referenced indices, other finding aids, and a sophisticated computerized retrieval system’ in order to make it more accessible to potential users”); *Judicial Watch, Inc. v. Dep’t of Justice*, 133 F. Supp. 2d 52, 53–54 (D.D.C. 2005) (finding Judicial Watch to be a news-media requester because it posted documents obtained through FOIA on its website).

The ACLU has also published a number of charts that collect, summarize, and analyze information it has obtained through FOIA. For example, through compilation and analysis of information gathered from various sources—including information obtained from the government through FOIA—the ACLU has created an original chart that provides the public and news media with a comprehensive index of Bush-era OLC memos relating to interrogation, detention, rendition, and surveillance. The chart describes what is publicly known about the memos and their conclusions, who authored them and for whom, and whether the memos remain secret or have been released to the public in whole or in part. It is *available at* http://www.aclu.org/safefree/general/olcmemos_chart.pdf. Similarly, the ACLU produced a chart of original statistics about the Defense Department’s use of NSLs based on its own analysis of records obtained through FOIA. That chart is *available at* http://www.aclu.org/safefree/nationalsecurityletters/released/nsl_stats.pdf. *See Nat’l Sec. Archive*, 880 F.2d at 1387 (explaining that the National Security Archive is a news-media requester because it obtained “documents for its own purpose, which is to assemble them, along with documents from other sources, into an encyclopedic work that it will then offer to the public”); *id.* (explaining that the National Security Archive is a news-media requester because it “gather[ed] information from a variety of sources; exercise[d] a significant degree of editorial discretion in deciding what documents to use and how to organize them; devise[d] indices and finding aids; and distribute[d] the resulting work to the public”).

The ACLU has also produced an in-depth television series on civil liberties called “The Freedom Files.” *See* <http://aclu.tv/>. The Freedom Files is a series of half-hour documentaries that features true stories about real people to highlight vital civil-liberties issues, and includes commentary and analysis from experts on particular civil-liberties problems; some portions also include explanation and analysis of information the ACLU has obtained through FOIA. *See* <http://aclu.tv/episodes>. In addition to distribution through the ACLU’s website, The Freedom Files series aired on Court TV, Link TV, and PBS stations nationwide. With each episode, the ACLU distributed fact sheets, reports, and FAQs. *See* <http://aclu.tv/educate>. The second season of The Freedom Files came with a teacher’s guide as well. *See* <http://aclu.tv/teachersguide>.

ACLU attorneys also frequently speak at conferences, before community groups and in academic settings.

In sum, the ACLU actively gathers news and information, analyzes it, creates distinct works, publishes that information, and disseminates it widely to the public. The ACLU plainly qualifies as an organization primarily engaged in the dissemination of information for FOIA's expedited processing purposes.

Courts have found organizations with missions similar to the ACLU's and that engage in information-dissemination activities similar to the ACLU's to be "primarily engaged in disseminating information." *See, e.g., Leadership Conference on Civil Rights*, 404 F. Supp. 2d at 260 (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"); *Am. Civil Liberties Union v. Dep't of Justice*, 321 F. Supp. 2d at 29 n.5 (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" (internal citation omitted)).¹¹

B. The requested records are urgently needed to inform the public about federal-government activity.

We make this Request primarily to retrieve cybersecurity-related documents regarding the extent to which communications providers share Americans' private information, including PII and the contents of communications, and other cybersecurity-related information, such as signatures, with the government, and the legal basis for those disclosures. To date, none of these documents have been made public.

President Obama's proposed cybersecurity package and other cybersecurity legislation now before Congress call for increased information

¹¹ Notably, other agencies routinely grant the ACLU's requests for expedited processing of FOIA requests, therefore recognizing that the ACLU is primarily engaged in disseminating information. In the past five years, the ACLU has been granted expedited processing by the Department of Commerce (August 2011), Office of Information Policy of the Department of Justice (August 2011, July 2011 and June 2011), the FBI (June 2011), the Office of Legal Counsel of the Department of Justice (June 2011), the National Security Division of the Department of Justice (June 2011 and May 2009), the Department of Justice (December 2008), the National Security Agency (October 2008), the Department of the Army (July 2006), the Defense Intelligence Agency (March 2006), the Civil Division of the Department of Justice (March 2006), and the Department of Justice's Office of Information and Privacy (January 1906).

sharing by the private sector with the government. Congress is intensely interested in these matters. There have been at least 14 Congressional hearings on cybersecurity in the last six months alone.¹² In addition to the cybersecurity legislative proposal put forth by the White House, no fewer than 17 cybersecurity bills have been introduced during the 112th Congress.¹³ Senate Majority Leader Harry Reid is pushing for the swift

¹² See *Cybercrime: Updating the Computer Fraud and Abuse Act to Protect Cyberspace and Combat Emerging Threats: Hearing Scheduled Before the S. Comm. on the Judiciary*, 112th Cong. (2011); *Cybersecurity: An Overview of Risks to Critical Infrastructure: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce*, 112th Cong. (2011); *Examining the Homeland Security. Impact of the Obama Administration's Cybersecurity Proposal: Hearing Before the Subcomm. on Cybersecurity, Infrastructure Protection and Sec. Technologies of the H. Comm. on Homeland Sec.*, 112th Cong. (2011); *Cybersecurity: Evaluating the Administration's Proposals: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 112th Cong. (2011); *Cybersecurity and Data Protection in the Financial Sector: Hearing Before the S. Comm. on Banking, Housing and Urban Affairs*, 112th Cong. (2011); *Cybersecurity: Assessing the Nation's Ability to Address the Growing Cyber Threat: Hearing Before the H. Comm. on Oversight and Gov't Reform*, 112th Cong. (2011); *Cybersecurity: Assessing the Immediate Threat to the United States: Hearing Before the Subcomm. on National Sec., Homeland Defense and Foreign Operations of the H. Comm. on Oversight and Gov't Reform*, 112th Cong. (2011); *Cybersecurity: Innovative Solutions to Challenging Problems: Hearing Before the Subcomm. on Intellectual Property, Competition and the Internet of the H. Comm. on the Judiciary*, 112th Cong. (2011); *Protecting Cyberspace: Assessing the White House Proposal: Hearing Before the S. Comm. on Homeland Sec. and Governmental Affairs*, 112th Cong. (2011); *Full Committee Hearing: to receive testimony on a joint staff Discussion Draft pertaining to cyber security of the bulk-power system and electric infrastructure and for other purposes: Hearing Before the S. Comm. on Energy and Natural Resources*, 112th Cong. (2011); *The Department of Homeland Security Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure: Hearing Before the Subcomm. on Cybersecurity, Infrastructure Protection and Sec. Technologies of the H. Comm. on Homeland Sec.*, 112th Cong. (2011); *Cyber Security: Responding to the Threat of Cyber Crime and Terrorism: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 112th Cong. (2011); *Examining the Cyber Threat to Critical Infrastructure and the American Economy: Hearing Before the Subcomm. on Cybersecurity, Infrastructure Protection and Sec. Technologies of the H. Comm. on Homeland Sec.*, 112th Cong. (2011).

¹³ See, e.g., Cybersecurity Education Enhancement Act of 2011, H.R. 76, 112th Cong. (2011); Homeland Security Cyber and Physical Infrastructure Protection Act of 2011, H.R. 174, 112th Cong. (2011); Executive Cyberspace Coordination Act of 2011, H.R. 1136, 112th Cong. (2011); Cybersecurity Enhancement Act of 2011, H.R. 2096, 112th Cong. (2011); SAFE Data Act, H.R. 2577, 112th Cong. (2011); Data Accountability and Trust Act (DATA) of 2011, H.R. 1841, 112th Cong. (2011); Tough and Smart National Security Act, S. 8, 112th Cong. (2011); Cybersecurity and Internet Safety Standards Act, S. 372, 112th Cong. (2011); Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. (2011); Cyber Security and American Cyber Competitiveness Act of 2011, S. 21, 112th Cong. (2011); Cyber Security Public Awareness Act of 2011, S. 813, 112th Cong. (2011); Cybersecurity Enhancement Act of 2011, S. 1152, 112th Cong. (2011); Cyberspace Warriors Act of 2011, S. 1159, 112th Cong. (2011); Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011); Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Cong. (2011); Information Technology Investment Management Act of 2011, S. 801, 112th Cong. (2011).

enactment of cybersecurity legislation and has secured the agreement of Republicans to a bi-partisan drafting process.¹⁴ Speaker of the House John Boehner and House Majority Leader Eric Cantor have appointed a Cybersecurity Task Force, due to report back in October 2011.¹⁵ But legislation is moving forward in the interim. Cybersecurity legislation passed the House Committee on Science, Space, and Technology on July 21, 2011, and is expected to go to the floor of the full House after the August recess.¹⁶ Therefore, time is of the essence; national debate about cybersecurity issues cannot fully take place without information as to the *current* extent of data sharing by the private sector with the government. The request for expedited processing should be granted.

The proposed bills and the government's policies with respect to cybersecurity, the extent to which government policies incorporate and reflect privacy concerns, have been the subject of intense media attention. *See, e.g.*, Somini Sengupta, *U.S. Agents, an Aerial Snoop and Teams of Hackers*, N.Y. Times, Aug. 7, 2011, <http://nyti.ms/qcpj34>; Adam Rawnsley, *Can Darpa Fix the Cybersecurity 'Problem from Hell?'*, WIRED Danger Room Blog, Aug. 5, 2011, <http://bit.ly/nXtc6Q>; Tabassum Zakaria, *Pentagon Cyber Program to Fund Hacker Innovation*, Reuters, Aug. 4, 2011, <http://reut.rs/oTgjFQ>; John D. Sutter, *Department of Defense Tries to Court Hackers*, CNN, Aug. 4, 2011, <http://bit.ly/ruStcY>; Marlene Cimon, *The Science of Cyber Security*, U.S. News & World Rep., Aug. 4, 2011, <http://bit.ly/nPVjfn>; *Communicators with Howard Schmidt*, C-SPAN, Aug. 2, 2011, <http://cs.pn/riQfZ0>; Adam Clark Estes, *The NSA Wants More Hackers for Their 'Collection of Geeks'*, The Atlantic Wire, Aug. 2, 2011, <http://bit.ly/plZ6jv>; Brendan Sasso & Gautham Nagesh, *Senators Unveil International Cybercrime Bill*, The Hill Tech. Blog, Aug. 2, 2011, <http://bit.ly/mY27nK>; *Herding Cats: Democratic Senators Introduce Cybersecurity Bills as Reid Tries to Consolidate Efforts*, Infosecurity, July 29, 2011, <http://bit.ly/oHXHpT>; Jim Finkle, *U.S. Government Says Stuxnet Could Morph into New Threat*, Reuters, July 28, 2011, <http://reut.rs/nJZJS3>; Diane Bartz, *Reid Pushes US Republicans for Cybersecurity Bill*, Reuters, July 27, 2011, <http://reut.rs/pWyvkW>; Robert Burns, *Army Chief Sees Cybersecurity as "Defining Issue"*, Associated Press, July 26, 2011, available at <http://onforb.es/o6vQT5>; Fahmida Y. Rashid, *U.S. Officials Tell Congress the Country Lags in Fortifying IT Security*, eWeek, July 26, 2011,

¹⁴ Diane Bartz, *Reid Pushes US Republicans for Cybersecurity Bill*, Reuters, Jul. 27, 2011, <http://reut.rs/rmOVbH>.

¹⁵ Press Release, Speaker of the House John Boehner, Speaker Boehner & Leader Cantor Announce New Cybersecurity Task Force Led by Rep. Thornberry (Jun. 24, 2011), <http://bit.ly/juTvN2>.

¹⁶ Josh Smith, *House Panel Approves Cybersecurity Standards Bill*, Nat'l J., July 21, 2011, <http://bit.ly/os2tW6>. There is a companion bill, S. 1152 before the Senate Committee on Commerce, Science and Transportation.

<http://bit.ly/nfbpPi>; Gautham Nagesh, *Cyber-Attacks on US Grow, Experts Say*, The Hill Tech. Blog, July 26, 2011, <http://bit.ly/oXHBvd>; Elizabeth Montalbano, *DOD Website Sells Public on Cybersecurity Strategy*, InformationWeek, July 25, 2011, <http://bit.ly/py2k38>; Ellen Nakashima, *GAO Faults Pentagon Cyber Efforts*, Wash. Post, July 25, 2011, <http://wapo.st/ppe3ma>; Micah Zenko, *Cyber Attacks and Pentagon Responses*, Council on Foreign Rel. Blog, July 25, 2011, <http://on.cfr.org/nOlyx7>; Sens. Joe Lieberman, Susan Collins, and Tom Carper, Letter to the Editor, *A Cyberspace Office at the White House*, Wash. Post, July 23, 2011, <http://wapo.st/plfBvH>; Jeanna Smialek, *Michael McCaul's Cybersecurity Bill Moves Forward*, Hous. Chron. Texas on the Potomac Blog, July 21, 2011, <http://bit.ly/oaEGZx>; Josh Smith, *House Panel Approves Cybersecurity Standards Bill*, Nat'l J., July 21, 2011, <http://bit.ly/qV3gGz>; Laura Crimaldi, *Nation's Fight Against Cyber Intruders Goes Local*, Associated Press, July 20, 2011, <http://bit.ly/nvu7aI>; David Lerman, *Senators Demand Answers on U.S. Cyber Warfare Policy*, Bloomberg, July 20, 2011, <http://bloom.bg/oEQlrw>; John T. Bennett, *Senators: US needs to Define Acts of Cyberwar*, The Hill Tech. Blog, July 19, 2011, <http://bit.ly/ovjBdR>; John T. Bennett, *McCain: White House, Pentagon Must Clarify Military's Cyber Role*, The Hill, July 19, 2011, <http://bit.ly/mU07RN>; Ben Pershing, *On Cybersecurity, Congress Can't Agree on Turf*, Wash. Post, July 18, 2011, <http://wapo.st/qB9bA5>; Jennifer Martinez, *DOD Could Use Force in Cyber War*, Politico, July 15, 2011, <http://politi.co/oxUnsf>; Rep. Jim Langevin, Letter to the Editor, *Beefing Up the Nation's Cybersecurity System*, Wash. Post, July 15, 2011, <http://wapo.st/qGQosC>; Julian E. Barnes & Siobhan Gorman, *Cyberwar Plan Has New Focus on Deterrence*, Wall St. J., July 15, 2011, <http://on.wsj.com/oDi9mr>; Tom Gjelten, *Pentagon Strategy Prepares for War in Cyberspace*, Nat'l Public Radio, July 15, 2011, <http://n.pr/o3UoQP>; Diane Bartz, *Key Senator Calls for Special Cyber Security Panel*, Reuters, July 13, 2011, <http://reut.rs/pqBaqx>; Kevin Baron, *Cyber Strategy: Take a More Active Role in Preventing Attacks*, Stars and Stripes, July 14, 2011, <http://1.usa.gov/qf2zh1>; *Pentagon Releases Cyber Security Strategy*, Fox News, July 14, 2011, <http://bit.ly/piYFXd>; Larisa Epatko, *Quick Take: The Pentagon's Cybersecurity Plan*, Pub. Broadcasting Service, July 14, 2011, <http://to.pbs.org/pqjynn>; Staff Writers, *McCain Calls for Special Cybersecurity Panel*, Agence France-Presse, July 13, 2011, <http://bit.ly/nR26nI>; Ellen Nakashima, *Pentagon to Unveil Cybersecurity Strategy*, Wash. Post, July 13, 2011, <http://wapo.st/orwnKs>; Catherine Hollander, *Lieberman, Collins, Carper Seek 'Gold Standard' in Cybersecurity*, Nat'l J., July 8, 2011, <http://bit.ly/ooQh6D>; Josh Smith, *Homeland Security Official: Some Foreign-Made Electronics Compromise Cybersecurity*, Nat'l J., July 7, 2011, <http://bit.ly/o8936x>; Jennifer Martinez, *Dem: Cybersecurity is Not a Partisan Issue*, Politico, June 29, 2011, <http://politi.co/pHOIIf>; Lolita Baldor, *Pentagon Gets Cyberwar Guidelines*, Associated Press, June 22, 2011, <http://fxn.ws/oIuUtR>; Larry Dignan, *Ex-*

DHS Chief Warns of Cyberwar with Hackers, CBS News, June 22, 2011, <http://bit.ly/o8IUXJ>; *String of Cyber Attacks Threat to U.S. Security?*, CBS News, June 20, 2011, <http://bit.ly/q5G0Bb>; Anna Mulrine, *CIA Chief Leon Panetta: The Next Pearl Harbor Could Be a Cyberattack*, Christian Science Monitor, June 9, 2011, <http://bit.ly/rdLYHr>; Tom Vanden Brook, *Panetta: Cyberattacks Among 'Blizzard' of Defense Challenges*, USA Today, June 9, 2011, <http://usat.ly/p2BFVs>; Paisley Dodds & Raphael G. Satter, *International law Covers Threats, Cyber Chief Says*, Associated Press, June 2, 2011, <http://bo.st/nu0NOg>; Hannah Northey, *Lawmakers Taking on Cyber Attacks, Nuclear Threats*, N.Y. Times, June 1, 2011 <http://nyti.ms/rpZI1k>; *US Pentagon to Treat Cyber-Attacks as 'Acts of War'*, BBC News, June 1, 2011, <http://bbc.in/n5Q5dY>; Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, Wall. St. J., May 31, 2011, <http://on.wsj.com/qDnAo1>; David E. Sanger & Elisabeth Bumiller, *Pentagon to Consider Cyberattacks Acts of War*, N.Y. Times, May 31, 2011, <http://nyti.ms/noJkd0>; Grant Gross, *Lawmakers Question Obama Cybersecurity Proposal*, PC World, May 25, 2011, <http://bit.ly/mSquwV>; Josh Smith, *House Panel Worries That Obama Cybersecurity Plan Could Open Door to Abuse*, Nat'l J., May 25, 2011, <http://bit.ly/k16y8Z>; Gautham Nagesh, *Cybersecurity Debate Shifts to House*, The Hill Tech. Blog, May 24, 2011, <http://bit.ly/o2tWB8>; Josh Smith, *Lawmakers Express Optimism, Concerns Over White House Cybersecurity Plan*, Nat'l J., May 24, 2011, <http://bit.ly/lpzhG7>; Lisa Daniel, *Pentagon, Homeland Security Collaborate on Cybersecurity*, Am. Forces Press Service, May 23, 2011, <http://1.usa.gov/oDi0tz>; Helene Cooper, *U.S. Calls for Global Cybersecurity Strategy*, N.Y. Times, May 16, 2011, <http://nyti.ms/pfAWQF>; Ellen Nakashima, *Obama Administration Outlines International Strategy for Cyberspace*, Wash. Post, May 16, 2011, <http://wapo.st/oxA4hF>; Ellen Nakashima, *White House Reveals Cybersecurity Plan*, Wash. Post, May 12, 2011, <http://wapo.st/niLRPl>; Lolita C. Baldor, *White House Unveils Cybersecurity Plan*, Associated Press, May 12, 2011, <http://usat.ly/mQpY2z>; Chloe Albanesius, *White House Unveils Cyber-Security Plan*, PC Mag, May 12, 2011, <http://bit.ly/lOMWwz>; Marc Ambinder, *White House Issues Major Cybersecurity Guidelines*, Nat'l J., May 12, 2011, <http://bit.ly/kArLdH>; Mary Beth Marklein, *Survey: Educators Lack Training to Teach Online Safety*, USA Today, May 4, 2011, <http://usat.ly/q8Z2pY>; *US Lacks People, Authorities to Face Cyber Attack*, Associated Press, March 16, 2011, <http://fxn.ws/qjwS8x>; Gopal Ratnam & Rachael King, *Pentagon Seeks \$500 Million for Cyber Technologies*, Bloomberg, Feb. 15, 2011, <http://bloom.bg/pp1yK3>; Richard A. Serrano, *U.S. Intelligence Officials Concerned about Cyber Attack*, L.A. Times, Feb. 11, 2011, <http://lat.ms/nLQiQL>; Jason Ryan, *CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor*, ABC News, Feb. 11, 2011, <http://abcn.ws/pO93qW>.

The disclosure of PII and other critical information held in governmental and corporate computer systems has also generated significant concern among the public and widespread and exceptional media attention, demonstrating the strong privacy interests at stake. *See, e.g.*, Michael Joseph Gross, *Enter the Cyber-Dragon*, Vanity Fair, Sept. 2011, <http://vntv.fr/qSbJS6>; Julia Angwin, *Latest in Web Tracking: Stealthy 'Supercookies'*, Wall St. J., Aug. 18, 2011, <http://on.wsj.com/r7xFSf>; Nicholas Jackson, *The Next Online Privacy Battle: Powerful Supercookies*, The Atlantic Tech. Blog, Aug. 18, 2011, <http://bit.ly/nXWfn1>; Jasmin Melvin, *Congresswoman Eyes McAfee Briefing on Cyber Attacks*, Reuters, Aug 10, 2011, <http://reut.rs/o4jjbx>; Jim Finkle, *Hackers Don't Need Movie Magic to Wreak Havoc*, Reuters, Aug. 6, 2011, <http://reut.rs/nJB1rr>; David Sarno, Salvador Rodriguez & Ken Dilanian, *Hackers Infiltrate Computer Networks of Thousands of Companies*, L.A. Times, Aug. 4, 2011, <http://lat.ms/q8fnVr>; David Goldman, *Countries Brace for The Code War*, CNN, Aug. 4, 2011, <http://cnmmon.ie/o4nn09>; Somini Sengupta, *Guardians of Internet Security are Targets*, N.Y. Times, Aug. 4, 2011, <http://nyti.ms/o6ANr4>; Jeremy A. Kaplan, *U.S. Cybercops Caught Flat-Footed by Massive Global Cyberattack*, Fox News, Aug. 4, 2011, <http://fxn.ws/nO0qC5>; David Barboza & Kevin Drew, *Security Firm Sees Global Cyberspying*, N.Y. Times, Aug. 3, 2011, <http://nyti.ms/pFA3vc>; Barbara Ortutay, *Report: Global Cyberattack Under Way for 5 years*, Associated Press, Aug 3, 2011, available at <http://bit.ly/oo7hYX>; Salvador Rodriguez, *Cyber Crimes are More Common and More Costly, Study Finds*, L.A. Times, Aug. 3, 2011, <http://lat.ms/nSepUY>; *Massive Global Cyberattack Targeting U.S., U.N. Discovered; Experts Blame China*, Fox News, Aug. 3, 2011, <http://fxn.ws/mYBF34>; Joseph Menn, *Cyberattacks Penetrate Military Secrets and Designs*, Fin. Times, Aug. 3, 2011, <http://on.ft.com/nuqJsC>; Jim Finkle, *"State Actor" Behind Slew of Cyber Attacks*, Reuters, Aug. 3, 2011, <http://reut.rs/o1ZrDQ>; Michael Joseph Gross, *Operation Shady Rat—Unprecedented Cyber-Espionage Campaign and Intellectual-Property Bonanza*, Vanity Fair, Aug. 2, 2011, <http://vntv.fr/qGq4fi>; Ellen Nakashima, *Report on 'Operation Shady RAT' Identifies Widespread Cyber-Spying*, Wash. Post, Aug. 2, 2011, <http://wapo.st/q0A1IU>; *Data-Breach Disclosures May Decline 50% Under Proposed Bills*, Bloomberg, Aug. 1, 2011, <http://bit.ly/nDulC9>; David Goldman, *China vs. U.S.: The Cyber Cold War is Raging*, CNN, July 28, 2011, <http://cnmmon.ie/pa547s>; David Goldman, *The Cyber Mafia Has Already Hacked You*, CNN, July 27, 2011, <http://cnmmon.ie/p6CPbq>; David Goldman, *Low-Tech Internet Scams Harvest Billions of Dollars*, CNN, July 26, 2011, <http://cnmmon.ie/pqjOVD>; David Goldman, *LulzSec and Anonymous are the Least of your Hacker Worries*, CNN, July 25, 2011, <http://cnmmon.ie/qxizXM>; Tom Gjelten, *Pentagon Strategy Prepares for War in Cyberspace*, Nat'l Pub. Radio, July 15, 2011, <http://n.pr/o3UoQP>; Thom Shanker & Elisabeth Bumiller, *Hackers Gained Access to Sensitive Military Files*, N.Y. Times, July 14, 2011, <http://nyti.ms/niiJde>; David

Alexander, *Cyber Theft Illustrates Pentagon Security Challenge*, Reuters, July 14, 2011, <http://reut.rs/qXFikW>; Lolita C. Baldor & Robert Burns, *Pentagon Discloses Massive Cyber Theft*, Associated Press, July 14, 2011, <http://on.msnbc.com/oFsWVU>; Salvador Rodriguez, *Attacks on Websites Spark Demand for Cyber-Security Experts*, L.A. Times, July 5, 2011, <http://lat.ms/mR55gQ>; *String of Cyber Attacks Threat to U.S. Security?*, CBS News, June 20, 2011, <http://bit.ly/q5G0Bb>; Ellen Nakashima, *CIA Web Site Hacked; Group LulzSec Takes Credit*, Wash. Post, June 15, 2011, <http://wapo.st/nLXRvp>; Howard Schneider & Ellen Nakashima, *IMF Investigates Suspected Attack on its Computers*, Wash. Post, June 11, 2011, <http://wapo.st/qwDPo4>; Ari Zoldan, *Cyber-Attacks Keep Coming -- Are We Really Prepared?*, Fox News, June 9, 2011, <http://fxn.ws/pNSXw6>; Raphael G. Satter, *Spotlight Falls on Sony's Troubled Cybersecurity*, Associated Press, June 3, 2011, <http://usat.ly/nEqsRv>; Byron Acohido, *Gmail Hit by Cyberattacks from China*, USA TODAY, June 2, 2011, <http://abcn.ws/n2hwGO>; David Goldman, *Massive Gmail Phishing Attack Hits Top U.S. Officials*, CNN, June 2, 2011, <http://cnnmon.ie/qmrlH4>; Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, Wall St. J., May 31, 2011, <http://on.wsj.com/qDnAo1>; David E. Sanger & Elisabeth Bumiller, *Pentagon to Consider Cyberattacks Acts of War*, N.Y. Times, May 31, 2011, <http://nyti.ms/oW4sZ7>; Daniel J. Solove, *Why "Security" Keeps Winning Out Over Privacy*, Salon, May 31, 2011, <http://bit.ly/pgK66j>; Chip Cutter & Lolita C. Baldor, *Lockheed Attack Highlights Rise in Cyber Espionage*, Associated Press, May 30, 2011, <http://bit.ly/pGo7dU>; *Sony: Data Breach was 'Sophisticated Cyber-Attack'*, Newsday, May 4, 2011, <http://bit.ly/qHtfAi>; Byron Acohido, *iPhone, Android Location-Logging Feature Sparks Privacy Concerns*, USA Today, Apr. 25, 2011, <http://usat.ly/qIRVeJ>; *Targeted Cyber Attacks to Rise in 2011, Security Experts Say*, Reuters, Apr. 5, 2011, <http://fxn.ws/owAadH>; *Did the Internet Kill Privacy?*, CBS News, Feb. 6, 2011, <http://bit.ly/p4GfSX>; Lisa Rein, *Hacker Breaches Security at Pentagon Federal Credit Union*, Wash. Post, Jan. 17, 2011, <http://wapo.st/pqJuFz>; Erik Larson, *U.S. Twitter Subpoena is Harassment, Lawyer Says*, Bloomberg, Jan. 10, 2011, <http://bloom.bg/oyIRFg>; Ryan Singel, *Twitter Response to WikiLeaks Subpoena Should be the Industry Standard*, WIRED Threat Level Blog, Jan. 10, 2011, <http://bit.ly/n7lPpi>; Scott Thurm & Yukari Iwatani Kane, *Your Apps are Watching You*, Wall St. J., Dec. 17, 2010, <http://on.wsj.com/qPNnY4>; Tanzina Vega, *A Call for a Federal Office to Guide Online Privacy*, NY Times, Dec. 16, 2010, <http://nyti.ms/qtaHwt>; *Federal Agents Urged to 'Friend' People on Social Networks, Memo Reveals*, Fox News, Oct. 14, 2010, <http://fxn.ws/qbulbn>; Emily Steel & Jessica E. Vascellaro, *Facebook, MySpace Confront Privacy Loophole*, Wall St. J., May 21, 2010, <http://on.wsj.com/mZeE4x>.

Furthermore, expedited processing is warranted because the records requested relate to a "matter of widespread and exceptional media interest in

which there exist possible questions about the government's integrity which affect public confidence." 28 C.F.R. § 16.5(d)(1)(iv). The privacy protections of Americans and their effects is enshrined in the Constitution. How often the government can and does access Americans' private information and read our private messages, and what it then does with that information, directly implicates those Constitutional protections. The Obama Administration has made clear that cybersecurity must take into account fundamental rights. *See, e.g.*, President Barack Obama, Remarks by the President on the Middle East and North Africa (May 19, 2011), <http://1.usa.gov/ifwPC2>; Office of the President, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (May 2011), <http://1.usa.gov/luajv7> ("Our international cyberspace policy reflects our core commitments to fundamental freedoms, privacy, and the free flow of information." *Id.* at 5.); Secretary of State Hillary Rodham Clinton, Internet Rights and Wrongs: Choices & Challenges in a Networked World, Address (Feb. 15, 2011), <http://1.usa.gov/q040Wc>; Secretary of State Hillary Rodham Clinton, Remarks on Internet Freedom (Jan. 21, 2010), <http://1.usa.gov/oz3nKM>. Should the government overstep its powers, our democratic freedoms would be gravely imperiled and public confidence in our government shaken. The documents sought here will directly address just how our government currently incorporates privacy protections in its cybersecurity policies and practices.

Application for Waiver or Limitation of Fees

- A. *A waiver of search, review, and reproduction fees is warranted under 5 U.S.C. § 552(a)(4)(A)(iii); 32 C.F.R. § 286.28(d); 28 § 16.11(k)(1); 32 C.F.R. § 1700.6(b)(2); 6 C.F.R. § 5.11(k); 47 C.F.R. § 0.470(e)(1); and 15 C.F.R. § 4.11(k)(1).*

The ACLU requests a waiver of search, review, and reproduction fees on the grounds that disclosure of the requested records is in the public interest because it is likely to contribute significantly to the public understanding of the operations or activities of the United States government and is not primarily in the commercial interest of the requester. 5 U.S.C. § 552(a)(4)(A)(iii).

The ACLU makes this Request specifically to retrieve any and all documents relating to requests for and disclosures of customer or user records, personal information or personally identifiable information, contents of electronic communications, and cybersecurity-related signatures, by communications providers to the federal government, for cybersecurity purposes. In doing so, the ACLU seeks to further the public's understanding of the degree to which, in the name of cybersecurity, the government seeks access to our private information and messages, how

often communications providers disclose that information (with or without a request from the government), and how the government uses the information it collects. As the dozens of news articles cited above make clear, interest in cybersecurity, government practices in this sphere, and the disclosure of personal information is widespread and exceptional. Disclosure of the requested records will contribute significantly to public understanding of the operations and activities of the government.

Moreover, disclosure is not in the requester's commercial interest. Any information disclosed by the requesters 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.'" (citation omitted)); OPEN Government Act of 2007, Pub. L. No. 110-175, 121 Stat. 2524, § 2 (Dec. 31, 2007) (finding that "disclosure, not secrecy, is the dominant objective of the Act," but that "in practice, the Freedom of Information Act has not always lived up to the ideals of that Act").

B. A waiver of search and review fees is warranted under 5 U.S.C. § 552(a)(4)(A)(ii); 32 C.F.R. § 286.28(e)(7); 28 C.F.R. § 16.11(c)(1)-(3), (d)(1); 32 C.F.R. § 1700.6(i)(2); 6 C.F.R. § 5.11(d); 47 C.F.R. § 0.470(a)(2)(i); and 15 C.F.R. § 4.11(d)(1).

A waiver of search and review fees is warranted because the requester 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). The ACLU is a representative of the news media in that it is an organization "actively gathering news for an entity that is organized and operated to publish or broadcast news to the public," where "news" is defined as "information that is about current events or that would be of current interest to the public." 5 U.S.C. § 552(a)(4)(A)(ii)(II).

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. § 552(a)(4)(A)(ii); *see also Nat'l Sec. Archive*, 880 F.2d at 1387 (finding that an organization that "gathers information from a variety of sources," 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 the purposes of FOIA); *cf. Am. Civil Liberties Union v. Dep't of Justice*, 321 F. Supp. 2d at 30 n.5 (finding non-profit public interest group to be

“primarily engaged in disseminating information”). The ACLU is a “representative of the news media” for the same reasons that it is “primarily engaged in the dissemination of information.” *See 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 media” for purposes of FOIA).¹⁷ Indeed, the ACLU of Washington recently was held to be a “representative of the news media.” *Am. Civil Liberties Union of Wash. v. Dep’t of Justice*, 2011 WL 887731, at *10 (W.D. Wash. Mar. 10, 2011). For all the reasons discussed above, the information sought here meets the definition of “news.”

Accordingly, fees associated with the processing of the Request should be “limited to reasonable standard charges for document duplication.” 5 U.S.C. § 552(a)(4)(A)(ii)(II).

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

* * *

Pursuant to applicable statute and regulations, we expect a determination regarding expedited processing within ten calendar days. *See* 5 U.S.C. § 552(a)(6)(E)(ii)(I).

If this FOIA Request is denied in whole or in part, we ask that you justify all withholdings by reference to specific exemptions to the FOIA.

¹⁷ Based on these factors, fees associated with responding to FOIA requests are regularly waived for the ACLU as a “representative of the news media.” In August 2011, the Department of Commerce granted a fee waiver to the ACLU with respect to a request for documents relating to the power of the President to shut down or restrict access to the internet. In June 2011, the National Security Division of the Department of Justice granted a fee waiver to the ACLU with respect to a request for documents relating to the interpretation and implementation a section of the PATRIOT Act. In October 2010, the Department of the Navy granted a fee waiver to the ACLU with respect to a request for documents regarding the deaths of detainees in U.S. custody. In January 2009, the CIA granted a fee waiver with respect to the same request. In March 2009, the Department of State granted a fee waiver to the ACLU with respect to its request for documents relating to the detention, interrogation, treatment, or prosecution of suspected terrorists. Likewise, in December 2008, the Department of Justice granted the ACLU a fee waiver with respect to the same request. In May 2005, the Department of Commerce granted a fee waiver to the ACLU with respect to its request for information regarding the radio frequency identification chips in United States passports. In March 2005, the Department of State granted a fee waiver to the ACLU with respect to a request regarding the use of immigration laws to exclude prominent non-citizen scholars and intellectuals from the country because of their political views. Also, the Department of Health and Human Services granted a fee waiver to the ACLU with regard to a FOIA request submitted in August of 2004. In addition, the Office of Science and Technology Policy in the Executive Office of the President said it would waive the fees associated with a FOIA request submitted by the ACLU in August 2003. Finally, three separate agencies—the Federal Bureau of Investigation, the Office of Intelligence Policy and Review, and the Office of Information and Privacy in the Department of Justice—did not charge the ACLU fees associated with a FOIA request submitted by the ACLU in August 2002.

We also ask that you release all segregable portions of otherwise exempt material. We reserve the right to appeal a decision to withhold any information or to deny a waiver of fees.

Please be advised that because we are requesting expedited processing under DOJ implementing regulations section 16.5(d)(1)(ii) as well as section 16.5(d)(1)(iv), we are sending a copy of this letter to DOJ's Office of Public Affairs. Notwithstanding Ms. Schmalzer's determination, we look forward to your reply within 20 business days, as the statute requires under section 552(a)(6)(A)(I).

Thank you for your prompt attention to this matter.

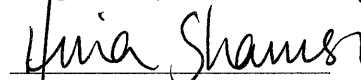
Please furnish the applicable records to:

Zachary Katznelson
American Civil Liberties Union Foundation
125 Broad Street 18th Floor
New York, NY 10004

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

I hereby affirm that the foregoing is true and correct to the best of my knowledge and belief. *See* 5 U.S.C. § 552(a)(6)(E)(vi).

Respectfully submitted,



HINA SHAMSI

American Civil Liberties Union Foundation
125 Broad St. 18th Floor
New York, NY 10004
Tel. 212-549-7321
Fax. 212-549-2654