epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

DEPARTMENT OF HOMELAND SECURITY

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-024 CBP Intelligence Records System (CIRS) System of Records

Notice of Proposed Rulemaking and Notice of new Privacy Act System of Records

[Docket No. DHS-2017-0026 and 0027]

October 23, 2017

By notice published September 21, 2017, the Department of Homeland Security ("DHS")/Customs and Border Protection (CBP) proposes to establish a new Privacy Act system of records titled "DHS/CBP-024 CBP Intelligence Records System (CIRS)."[1] The system of records notice ("SORN") proposes numerous routine use disclosures.[2] This new database will contain records containing names, Social Security numbers, passport information, immigration benefit data, public-source data—including social media information—reports of suspicious activities, and metadata.[3] The individuals covered by the database include individuals associated with CBP investigations (e.g. witnesses), individuals identified in classified or unclassified intelligence reports, individuals identified in immigration benefit data, and individuals identified

[1] Systems of Record Notice, 82 Fed. Reg. 44,198 (Sept. 21, 2017) (hereafter "CIRS SORN").
[2] *Id.* at 44,201-202.
[3] *Id.* at 44,200-201.

in public news reports.[4] The scope of the individuals subject to the database and the scope of the information to be contained in the database are both broad and ambiguous.

By notice published September 21, 2017, DHS published a notice of public rulemaking ("NPRM") that proposes to exempt the CIRS database from several significant provisions of the Privacy Act of 1974.[5] Pursuant to DHS's notices, the Electronic Privacy Information Center ("EPIC") submits these comments to: (1) underscore the substantial privacy and security issues raised by the database; (2) recommend CBP withdraw unlawful and unnecessary proposed routine use disclosures; (3) recommend the CBP to significantly narrow their Privacy Act exemptions; (4) urge CBP to withdraw the agency's proposal to add social media information to the database; and (5) advocate for the review of the CBP's use and analysis of social media information.

I. EPIC's Interest

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and protect privacy, the First Amendment, and constitutional values.[6] EPIC has a particular interest in preserving privacy safeguards, established by Congress, in the development of new information systems operated by the federal government and ensuring the right of people to engage in First Amendment protected activities without the threat of government surveillance.

EPIC previously sued the Department of Homeland Security ("DHS") to obtain documents related to a DHS social network and media monitoring program.[7] These documents revealed that the agency had paid over $11 million to an outside company, General Dynamics, to

[4] *Id.* at 44,200.
[5] Notice of Proposed Rulemaking, 82 Fed. Reg. 44,124 (Sept. 21, 2017) (hereafter "CIRS NPRM").
[6] EPIC, *About EPIC* (2016), https://epic.org/epic/about.html.
[7] EPIC, *EPIC v. Department of Homeland Security: Media Monitoring*, https://epic.org/foia/epic-v-dhs-media-monitoring/.

engage in monitoring of social networks and media organizations and prepare summary reports for DHS.[8] According to DHS documents, General Dynamics would "monitor public social communications on the Internet," including the public comments sections of NYT, LA Times, Huff Po, Drudge, Wired's tech blogs, and ABC News.[9] DHS also requested monitoring of Wikipedia pages for changes[10] and announced its plans to set up social network profiles to monitor social network users.[11]

DHS required General Dynamics to monitor not just "potential threats and hazards" and "events with operational value," but also paid the company to "identify[] media reports that reflect adversely on the U.S. Government [or] DHS . . . ."[12] DHS clearly intended to "capture public reaction to major government proposals."[13] DHS instructed the media monitoring company to generate summaries of media "reports on DHS, Components, and other Federal Agencies: positive and negative reports on FEMA, CIA, CBP, ICE, etc. as well as organizations outside the DHS."[14]

The documents obtained by EPIC through its Freedom of Information Act lawsuit led to a Congressional hearing on DHS social network and media monitoring program.[15] EPIC submitted a statement for the record for that hearing opposing the agency's media monitoring and called for

[8] DHS Social Media Monitoring Documents, *available at* https://epic.org/foia/epic-v-dhs-media-monitoring/EPIC-FOIA-DHS-Media-Monitoring-12-2012.pdf; *See also* Charlie Savage, *Federal Contractor Monitored Social Network Sites*, New York Times, Jan. 13, 2012, http://www.nytimes.com/2012/01/14/us/federal-security-program-monitored-public-opinion.html.
[9] DHS Social Media Monitoring Documents, *supra* note 6, at 127, 135, 148, 193.
[10] *Id.* at 124, 191.
[11] *Id.* at 128.
[12] *Id.* at 51, 195.
[13] *Id.* at 116.
[14] *Id.* at 183, 198.
[15] *See DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy: Hearing Before the Subcomm. on Counterterrorism and Intelligence of the H. Comm. on Homeland Security*, 112th Cong. (2012).

the immediate end of the program.[16] Members of Congress expressed concern about the federal agency's plan to monitor social media.[17]

Given government misuse of social media monitoring techniques in the past, EPIC is skeptical of CBP's proposal to add social media information to an intelligence database for scrutiny by the agency. EPIC opposes this proposal along with the vast routine use disclosures and exemptions from the Privacy Act that CBP is claiming.

II. The CIRS Database Would Maintain a Massive Amount of Personal, Sensitive Information About a Wide Variety of Individuals

a. Categories of Records in the CBP Database Are Virtually Unlimited

According to the CIRS system of record notice, the CIRS database will include an exorbitant amount of personal information about an expansive array of individuals. The categories of records contained in the CIRS database represent a wealth of sensitive information that should be afforded the highest degree of privacy and security protections, such as financial records[18] and Social Security Numbers.[19] The CIRS database will also include passport information, addresses, phone numbers, immigration benefit data, information from other government databases, and information about confidential sources and informants. Federal contractors, security experts, and EPIC have argued to the U.S. Supreme Court that much of this information simply should not be collected by the federal government.

---

[16] Marc Rotenberg, President and Ginger McCall, EPIC Open Government Project Director, *Statement for the Record for Hearing on DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy* (Feb. 16, 2012), https://epic.org/privacy/socialmedia/EPIC-Stmnt-DHS-Monitoring-FINAL.pdf.
[17] Andrea Stone, *DHS Monitoring of Social Media Under Scrutiny by Lawmakers,* Huffington Post, Feb. 16, 2012, http://www.huffingtonpost.com/2012/02/16/dhs-monitoring-of-social-media_n_1282494.html; *Congress Grills Department of Homeland Security,* EPIC, Feb. 16, 2012, https://epic.org/2012/02/congress-grills-department-of-.html.
[18] *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered section of 12 and 15 U.S.C.).
[19] *See* Driver's Privacy Protection Act, 18 U.S.C. § 2725(4) (defining "highly restricted personal information" to include "social security number").

In *NASA v. Nelson*,[20] the Supreme Court considered whether federal contract employees have a Constitutional right to withhold personal information sought by the government in a background check. EPIC filed an amicus brief, signed by 27 technical experts and legal scholars, siding with the contractors employed by the Jet Propulsion Laboratory ("JPL").[21] EPIC's brief highlighted problems with the Privacy Act, including the "routine use" exception, security breaches, and the agency's authority to carve out its own exceptions to the Act.[22] EPIC also argued that compelled collection of sensitive data would place at risk personal health information that is insufficiently protected by the agency.[23] The Supreme Court acknowledged that the background checks implicate "a privacy interest of Constitutional significance" but stopped short of limiting data collection by the agency, reasoning that the personal information would be protected under the Privacy Act.[24]

That turned out not to be true. Shortly after the Court's decision, NASA experienced a significant data breach that compromised the personal information of about 10,000 employees, including Robert Nelson, the JPL scientist who sued NASA over its data collection practices.[25] The JPL-NASA breach is a clear warning about why CBP should narrow the amount of sensitive data collected. Simply put, the government should not collect so much data; to do so unquestionably places people at risk.

Given the recent surge in government data breaches, the sensitive information contained in the CIRS database faces significant risk of compromise. According to a recent report by the U.S. Government Accountability Office ("GAO"), "[c]yber-based intrusions and attacks on

[20] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134 (2011).
[21] Amicus Curiae Brief of EPIC, *Nat'l Aeronautics & Space Admin. v. Nelson*, No. 09-530 (S.Ct. Aug. 9, 2010), https://epic.org/amicus/nasavnelson/EPIC_amicus_NASA_final.pdf.
[22] *Id*. at 20-28
[23] *Id*.
[24] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134, 147 (2011).
[25] Natasha Singer, *Losing in Court, and to Laptop Thieves, in a Battle With NASA Over Private Data*, N.Y. TIMES (Nov. 28, 2012), http://www.nytimes.com/2012/11/29/technology/ex-nasa-scientists-data-fears-come-true.html.

federal systems have become not only more numerous and diverse but also more damaging and disruptive."[26] This is illustrated by the 2015 data breach at OPM, which compromised the background investigation records of 21.5 million individuals.[27] Also in 2015, the Internal Revenue Service ("IRS") reported that approximately 390,000 tax accounts were compromised, exposing Social Security Numbers, dates of birth, street addresses, and other sensitive information.[28] In 2014, a data breach at the U.S. Postal Service exposed personally identifiable information for more than 80,000 employees.[29]

The latest series of high-profile government data breaches indicates that federal agencies are incapable of adequately protecting sensitive information from improper disclosure. Indeed, GAO recently released a report on widespread cybersecurity weaknesses throughout the executive branch, aptly titled "Federal Agencies Need to Better Protect Sensitive Data."[30] According to the report, a majority of federal agencies "have weaknesses with the design and implementation of information security controls …."[31] In addition, most agencies "have weaknesses in key controls such as those for limiting, preventing, and detecting inappropriate access to computer resources and managing the configurations of software and hardware."[32] The GAO report concluded that, due to widespread cybersecurity weaknesses at most federal agencies, "federal systems and information, as well as sensitive personal information about the public, will be at an increased risk of compromise from cyber-based attacks and other threats."[33]

---

[26] U.S. Gov't Accountability Office, *DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System* (Jan. 2016) http://www.gao.gov/assets/680/674829.pdf (hereafter "GAO Cybersecurity Report").
[27] GAO Cybersecurity Report at 8.
[28] *Id*. at 7-8.
[29] *Id*. at 8.
[30] GAO Sensitive Data Protection Report.
[31] *Id*. at unpaginated "Highlights" section.
[32] *Id*.
[33] *Id*. at 12.

Data breaches have directly impacted DHS information systems in recent years. For example, in 2014, a DHS contractor conducting background investigations for the agency experienced a data breach that compromised the records of at least 25,000 employees, including undercover investigators.[34] In 2015, another DHS contractor suffered a data breach that affected as many as 390,000 people associated with DHS, including current and former employees as well as contractors and job applicants.[35] More recently, a 16-year-old teenage boy was arrested in connection with hacks that exposed the information of more than 20,000 Federal Bureau of Investigation ("FBI") employees and 9,000 DHS employees, as well as the personal email accounts of DHS Secretary Jeh Johnson and Central Intelligence Agency ("CIA") director John Brennan.[36] Overall, the number of government data breaches, including for DHS, has exploded in the last decade, rising from 5,503 in 2006 to 67,168 in 2014.[37]

These weaknesses in DHS databases increase the risk that unauthorized individuals could read, copy, delete, add, or modify sensitive information contained in the CIRS database. Accordingly, CBP should maintain only records that are relevant and necessary to an investigation. To the extent that CBP continues to collect this vast array of sensitive personal information, CBP should limit disclosure to only those agencies and government actors that require the information as a necessity. Further, CBP should strictly limit the use of this information to the purpose for which it was originally collected.

---

[34] Jim Finkle & Mark Hosenball, *U.S. Undercover Investigators Among Those Exposed in Data Breach*, REUTERS (Aug. 22, 2014), http://www.reuters.com/article/us-usa-security-contractor-cyberattack-idUSKBN0GM1TZ20140822.
[35] Alicia A. Caldwell, *390,000 Homeland Employees May Have Had Data Breached*, ASSOCIATED PRESS (June 15, 2015), http://www.pbs.org/newshour/rundown/390000-homeland-employees-may-have-had-data-breached/.
[36] Alexandra Burlacu, *Teen Arrested Over DHS and FBI Data Hack*, TECH TIMES (Feb. 13, 2016), http://www.techtimes.com/articles/133501/20160213/teen-arrested-over-dhs-and-fbi-data-hack.htm.
[37] U.S. Gov't Accountability Office, *Federal Agencies Need to Better Protect Sensitive Data* 4 (Nov. 17, 2015), http://www.gao.gov/assets/680/673678.pdf [hereinafter "GAO Sensitive Data Protection Report"].

There is also reason to be concerned about foreign governments compromising the CIRS database. Foreign governments continue to show a willingness to interfere with and infiltrate government agencies.[38] The ability for foreign government to access and provide information for the database is particularly concerning given recent revelations that foreign governments have been willing to provide false information that has the potential to derail investigations.[39]

b. CIRS Database Covers Broad Categories of Individuals and Implicates Individuals Who Are Not Under Investigation

The CBP proposes to collect the previously described personal data, including data on individuals who are not themselves under CBP investigation. The CIRS database would contain records on individuals merely associated with CBP investigations, including witnesses, associates, and informants; individuals who have reported suspicious activities, threats, or other incidents; and individuals identified in visa, immigration, or naturalization benefit data.[40]

By collecting, maintaining, and disclosing the records of such a broad variety of people, CBP could create detailed profiles of individuals who are not themselves the target of any investigation, do not work for the government, and who may be trying to aid CBP in carrying out their statutorily prescribed duties. Maintaining so much information and exempting it from Privacy Act protections will only serve to frustrate CBP operations as individuals may be unlikely to come forward with information about crimes or specific activity knowing that information may be kept about them personally. Furthermore, given ongoing concerns about data security, these individuals could effectively be placing themselves in significant danger if the

[38] Brian Ross & Pete Madden, *United States Remains Vulnerable to North Korean Cyber-Attack, Analysts Say,* ABC News, Apr. 22, 2017, http://abcnews.go.com/International/united-states-remains-vulnerable-north-korean-cyber-attack/story; David E. Sanger, *Putin Ordered 'Influence Campaign' Aimed at U.S. Election, Report Says,* New York Times, Jan. 6, 2017, https://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html.
[39] Karoun Demirjian & Devlin Barrett, *How a Dubious Russian Document Influenced the FBI's Handling of the Clinton Probe,* Washington Post, May 24, 2017, https://www.washingtonpost.com/world/national-security/how-a-dubious-russian-document-influenced-the-fbis-handling-of-the-clinton-probe/2017/05/24/f375c07c-3a95-11e7-9e48-c4f199710b69_story.html.
[40] CIRS SORN at 44,200.

database is breached and information about victims or witnesses who come forward are compromised.

III. Proposed Routine Uses Would Circumvent Privacy Act Safeguards and Contravene Legislative Intent

The Privacy Act's definition of "routine use" is precisely tailored, and has been narrowly prescribed in the Privacy Act's statutory language, legislative history, and relevant case law. The CIRS database contains a potentially broad category of personally identifiable information. By disclosing information in a manner inconsistent with the purpose for which the information was originally gathered, the CBP exceeds its statutory authority to disclose personally identifiable information without obtaining individual consent.

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and required agencies to be transparent in their information practices.[41] Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[42]

The Privacy Act prohibits federal agencies from disclosing records they maintain "to any person, or to another agency" without the written request or consent of the "individual to whom the record pertains."[43] The Privacy Act also provides specific exemptions that permit agencies to disclose records without obtaining consent.[44] One of these exemptions is "routine use."[45]

[41] S. Rep. No. 93-1183 at 1 (1974).
[42] Pub. L. No. 93-579 (1974).
[43] 5 U.S.C. § 552a(b).
[44] *Id*. §§ 552a(b)(1)–(12).
[45] *Id*. § 552a(b)(3).

"Routine use" means "with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected."[46]

The Privacy Act's legislative history and a subsequent report on the Act indicate that the routine use for disclosing records must be specifically tailored for a defined purpose for which the records are collected. The legislative history states that:

> [t]he [routine use] definition should serve as a caution to agencies to think out in advance what uses it will make of information. This Act is not intended to impose undue burdens on the transfer of information . . . or other such housekeeping measures and necessarily frequent interagency or intra-agency transfers of information. It is, however, intended to discourage the unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material.[47]

The Privacy Act Guidelines of 1975—a commentary report on implementing the Privacy Act— interpreted the above Congressional explanation of routine use to mean that a "'routine use' must be not only compatible with, but related to, the purpose for which the record is maintained."[48]

Subsequent Privacy Act case law limits routine use disclosures to a precisely defined system of records purpose. In *United States Postal Service v. National Association of Letter Carriers, AFL-CIO*, the Court of Appeals for the D.C. Circuit determined that "the term 'compatible' in the routine use definitions contained in [the Privacy Act] was added in order to limit interagency transfers of information."[49] The Court of Appeals went on to quote the Third Circuit and made clear, "[t]here must be a more concrete relationship or similarity, some

[46] 5 U.S.C. § 552a(a)(7).
[47] *Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).
[48] *Id*.
[49] *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, AFL-CIO*, 9 F.3d 138, 144 (D.C. Cir. 1993).

meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and in its disclosure."[50]

The CIRS SORN proposes numerous routine uses that are incompatible with the purpose for which the data was collected.[51] Proposed Routine Use J would permit CBP to disclose information:

> To an appropriate federal, state, local, tribal, foreign, or international agency, if the information is relevant and necessary to the agency's decision concerning the hiring or retention of an individual or the issuance, grant, renewal, suspension, or revocation of a security clearance, license, contract, grant, or other benefit. . . .[52]

Proposed Routine Use V would permit DHS to disclose information:

> To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy. [53]

The CBP proposes to disclose CIRS database information for purposes that do not relate to CBP investigations. Determinations regarding employment or licensing as contemplated by Routine Use J is entirely unrelated to this purpose. These routine uses directly contradict Congressman William Moorhead's testimony that the Privacy Act was "intended to prohibit gratuitous, ad hoc, disseminations for private or otherwise irregular purposes."[54]

---

[50] *Id*. at 145 (quoting *Britt v. Natal Investigative Serv*., 886 F.2d 544, 549-50 (3d. Cir. 1989). *See also Doe v. U.S. Dept. of Justice*, 660 F.Supp.2d 31, 48 (D.D.C. 2009) (DOJ's disclosure of former AUSA's termination letter to Unemployment Commission was compatible with routine use because the routine use for collecting the personnel file was to disclose to income administrative agencies); *Alexander v. F.B.I*, 691 F. Supp.2d 182, 191 (D.D.C. 2010) (FBI's routine use disclosure of background reports was compatible with the law enforcement purpose for which the reports were collected).
[51] CIRS SORN at 44,201.
[52] *Id*.
[53] *Id*. at 44,202.
[54] *Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).

CBP also proposes to create a "Public Relations" exemption to the Privacy Act through Routine Use V that would permit the agency to release personal information to the media or members of the general public if there was a "legitimate public interest" unless the CBP determines that it is an "unwarranted invasion of personal privacy."[55] This Routine Use is unnecessarily broad especially given the number of people to be included in the proposed database and threatens to mistakenly expose the personal information of individuals. CBP should remove this proposed Routine Use because creating a category that is too broad can easily lead to the abuse of privacy rights of individuals whose data has been gathered and stored by the CBP.

In addition, the proposed routine uses that would permit the CBP to disclose records, subject to the Privacy Act, to foreign, international, and private entities should be removed. The Privacy Act only applies to records maintained by United States government agencies.[56] Releasing information to private and foreign entities does not protect individuals covered by this records system from Privacy Act violations.

IV. The CBP Proposes Broad Exemptions for the CIRS Database, Contravening the Intent of the Privacy Act of 1974

CBP proposes to exempt the CIRS database from key Privacy Act obligations, such as the requirement that records be accurate and relevant, or that individuals be allowed to access and amend their personal records.

When Congress enacted the Privacy Act in 1974, it sought to restrict the amount of personal data that federal agencies were able to collect.[57] Congress further required agencies to be transparent in their information practices.[58] In *Doe v. Chao*,[59] the Supreme Court underscored

[55] CIRS SORN at 44,202.
[56] 5 U.S.C. § 552a(b).
[57] S. Rep. No. 93-1183, at 1 (1974).
[58] *Id*.
[59] *Doe v. Chao*, 540 U.S. 614 (2004).

the importance of the Privacy Act's restrictions upon agency use of personal data to protect privacy interests, noting that "in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies."[60]

But despite the clear pronouncement from Congress and the Supreme Court on accuracy and transparency in government records, CBP proposes to exempt the Database from compliance with the following safeguards: 5 U.S.C. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g).[61] These provisions of the Privacy Act require agencies to:

- grant individuals access to an accounting of when, why, and to whom their records have been disclosed;[62]
- inform parties to whom records have been disclosed of any subsequent corrections to the disclosed records;[63]
- allow individuals to access and review records contained about them in the database and to correct any mistakes;[64]
- collect and retain only such records "about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President";[65]
- collect information from the individual to the greatest extent possible, when such information would have an adverse effect on the individual;[66]
- inform individuals from whom they request information the purposes and routine uses of that information, and the effect of not providing the requested information;[67]
- notify the public when it establishes or revises a database, and provide information on the categories of information sources and procedures to access and amend records contained in the database;[68]
- ensure that all records used to make determinations about an individual are accurate, relevant, timely and complete as reasonably necessary to maintain fairness;[69]

[60] *Doe*, 540 U.S. at 618.
[61] 81 Fed. Reg. 9789, 9790.
[62] 5 U.S.C. § 552a(c)(3).
[63] *Id.* § 552a(c)(4).
[64] *Id*. § 552a(d).
[65] *Id*. § 552a(e)(1).
[66] *Id*. § 552a(e)(2).
[67] *Id*. § 552a(e)(3).
[68] *Id*. § 552a(e)(4)(G), (H), (I).
[69] *Id*. § 552a(e)(5).

- serve notice to an individual whose record is made available under compulsory legal process;[70]
- create procedures to handle inquiries by individuals regarding the presence of information about them in a particular database;[71] and
- submit to civil remedies and criminal penalties for agency violations of the Privacy Act.[72]

Several of the CBP claimed exemptions would further exacerbate the impact of its overbroad categories of records and routine uses in this system of records. The CBP exempts itself from § 552a(e)(1), which requires agencies to maintain only those records relevant to the agency's statutory mission. The agency exempts itself from § 552a(e)(4)(I), which requires agencies to disclose the categories of sources of records in the system. And the agency exempts itself from its Privacy Act duties under § 552a(e)(4)(G) and (H), which allows individuals to access and correct information in its records system. In other words, the CBP claims the authority to collect any information it wants without disclosing where it came from or even acknowledging its existence. The net result of these exemptions, coupled with the CBP's proposal to collect and retain virtually unlimited information unrelated to any purpose Congress delegated to the agency, would be to diminish the accountability of the agency's information collection activities.

The CBP also proposes exemption from maintaining records with "such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination."[73] Essentially, the CBP admits that it contemplates collecting information that will not be relevant or necessary to a specific investigation. The agency claims that the inability to determine, in advance, whether information is accurate, relevant, timely, and complete precludes its agents from complying with the obligation to ensure that the information

[70] *Id.* § 552a(e)(8).
[71] *Id.* § 552a(f).
[72] *Id.* § 552a(g).
[73] 5 U.S.C. § 552a(e)(5).

meets these criteria after it is stored.[74] By implication, the agency objects to guaranteeing "fairness" to individuals in the CIRS database.

It is inconceivable that the drafters of the Privacy Act would have permitted a federal agency to maintain a database on U.S. citizens containing so much personal information and simultaneously be granted broad exemptions from Privacy Act obligations. It is as if the agency has placed itself beyond the reach of the American legal system on the issue of greatest concerns to the American public – the protection of personal privacy. Consistent and broad application of Privacy Act obligations are the best means of ensuring accuracy and reliability of database records, and the CBP must reign in the exemptions it claims for its CIRS database.

V. The CBP's Increasing Collection and Use of Social Media Threatens First Amendment Rights

The CBP's increasing focus on social media threatens to chill First Amendment protected rights and undermine online spaces as public forums of democratic debate. Over the past year, CBP has published a notice no less than three times with a proposal related to the collection and use of social media information by the agency. CBP proposed to add a question to I-94W (Nonimmigrant Visa Waiver Arrival/Departure Record) and to the Electronic System for Travel Authorization inquiring about an applicant's social media identifiers.[75] CBP proposed to add a similar question to the Electronic Visa Update System.[76] Most recently, CBP proposed to include social media identifiers and other social media information in the official immigration files of

[74] CIRS NPRM at 44,125.
[75] Notice and Request for Comments, 81 Fed. Reg. 40,892 (June 23, 2016).
[76] Notice of request for public comment on "Agency Information Collection Activities: Electronic Visa Update System," 82 Fed. Reg. 19,380 (Apr. 27, 2017).

individual's known as Alien Files or "A-Files."[77] The CBP now proposes to include social media information, including metadata, in a newly created intelligence database.

The CBP's Intelligence Reporting System poses a significant threat to the First Amendment and marginalized groups in particular. The CIRS database will not only collect social media information but use data mining tools to analyze the data. Specifically, CBP will use the Analytical Framework for Intelligence ("AFI") and the Intelligence Reporting System ("IRS") to analyze the data in CIRS.[78] The information CBP will be analyzing will largely be from "information initially collected by CBP pursuant to its immigration and customs authorities."[79]

CBP's proposal to collect social media information in an intelligence database implicates the First Amendment and will chill freedom's speech, expression, and association. These are core civil liberties and have been strongly protected by the Constitution and the U.S. courts.[80] These rights extend to non-U.S. citizens.[81]

Many people around the world use social media, including Facebook and Twitter, to support democratic movements and to campaign for political reform.[82] But these political views

[77] Notice of Modified Privacy Act System of Records "Privacy Act of 1974; System of Records," 82 Fed. Reg. 43,556 (Sept. 18, 2017).
[78] *See* CIRS NPRM at 44,124.
[79] *Id.*
[80] *See, e.g.*, *United States v. Stevens*, 130 S. Ct. 1577, 1585 (2010) (holding that the "First Amendment itself reflects a judgment by the American people that the benefits of its restrictions on the Government outweigh the costs"); *see also NAACP v. Alabama ex. rel. Patterson,* 357 U.S. 449 (1958) (holding that immunity from state scrutiny of membership lists was related to the right of freedom of association and fell under the 14th Amendment of the U.S. Constitution); *City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015) (holding that a city ordinance that required hotels to make their registries available to the police on demand was unconstitutional under the 4th Amendment of the U.S. Constitution).
[81] *See* David Cole, *Are Foreign Nationals Entitled to the Same Constitutional Rights as Citizens?*, 25 T. Jefferson L. Rev. 367-388 (2003) ("foreign nationals are generally entitled to the equal protection of the laws, to political freedoms of speech and association, and to due process requirements of fair procedure where their lives, liberty, or property are at stake.").
[82] Sophie Hutchinson, *Social media Plays Major Role In Turkey Protests,* BBC, Jun. 4, 2013, http://www.bbc.com/news/world-europe-22772352; David Auerbach, *The Bernie Bubble,* Slate, Feb. 17, 2016, http://www.slate.com/articles/technology/future_tense/2016/02/the_bernie_sanders_campaign_owes_a_lot_to_social_media.html.

reflect the specific circumstances of national political systems and regional political conflict, and there is some risk that comments taken out of context could discourage political reform efforts. For example, social media is credited with empowering the Arab Spring and allowing Egyptians to remove former President Hosni Mubarak from power.[83] Social media also played a pivotal role in the 2013 Gezi Park protests in Turkey and the recent anti-Putin protests in Russia, which were sparked by a blog post and YouTube video.[84]

CBP wants to obtain social media information and data mine it along with other information (much of the information from individuals not suspected of a crime) to create intelligence reports.[85] However, the proposal assumes that social media provides an accurate picture of a person and those they are close with. People connect with others on social media for many reasons. An individual's "friend" on a social media site could range from a close friend to an acquaintance to someone they may never have met. Often individuals connect to people on social media who have completely different perspectives and world views. Furthermore, the proposal fails to state to what extent possible social media associations will be used in the intelligence reporting to make determinations about whether individuals pose a threat.

The proposal also fails to explain how CBP will use social media information and metadata in identifying individuals that pose a national security or public safety threat. Many individuals have been on social media for years and have created a permanent record of their

[83] Amitava Kumar, *'Revolution 2.0': How Social Media Toppled A Dictator,* NPR, Feb. 8, 2012, http://www.npr.org/2012/02/08/145470844/revolution-2-0-how-social-media-toppled-a-dictator; Ramesh Srinivasan, *Taking Power Through Technology in the Arab Spring,* Al Jazeera, Oct. 26, 2012, http://www.aljazeera.com/indepth/opinion/2012/09/201291911534429984 8.html.
[84] Steve Dorsey, *Turkey's Social Media And Smartphones Key To 'Occupy Gezi' Protests,* Huffington Post, Jun. 10, 2013, http://www.huffingtonpost.com/2013/06/09/turkey-social-media-smartphones-occupy-gezi-protests_n_3411542.html; Julia Ioffee, *What Russia's Latest Protests Mean for Putin,* The Atlantic, Mar. 27, 2017, https://www.theatlantic.com/international/archive/2017/03/navalny-protests-russia-putin/520878/.
[85] *See* Notice of Proposed Rulemaking, 82 Fed. Reg. 44,124 (Sept. 21, 2017)

lives.[86] Teenagers are routinely warned to be careful of what they post on social media,[87] however teenagers as well as adults have made posts on social media which they later regret and may not be an actual reflection of who they are.[88] This should be taken into account when considering whether to use social media information to make any determinations about individuals. Social media does not necessarily reflect who a person truly is and taking posts out of context has the potential to wrongly deny people entry because of an inside joke or posturing that CBP does not understand from viewing certain information in isolation.[89] These problems identified above will only be exacerbated by the use of secret algorithms that analyze the data and make possibly life-impacting determinations about individuals.

Government programs that threaten important First Amendment rights are immediately suspect and should only be undertaken where the government can demonstrate a compelling interest that cannot be satisfied in other way.[90] Government programs that scrutinize online comments, dissent, and criticism for the purpose of trying to identify threats sends a chilling message to all users of social media—which increasingly provides important forums to share ideas, engage in debates, and explore new ideas.

Concern over the how the government uses social media is widespread and several questions remain unanswered. Earlier this year, several members of the House of Representatives

---

[86] Alexandra Mateescu et. al., *Social Media Surveillance and Law Enforcement*, DATA & CIVIL RIGHTS, Oct. 27, 2015, http://www.datacivilrights.org/pubs/2015-1027/Social_Media_Surveillance_and_Law_Enforcement.pdf.
[87] Franki Rosenthal, *Caution ahead: The dangers of social media*, SUN SENTINEL, Feb. 2, 2016, http://www.sun-sentinel.com/teenlink/college/tl-caution-ahead-the-dangers-of-social-media-20160202-story.html.
[88] Alyssa Giacobbe, *6 ways social media can ruin your life*, BOSTON GLOBE, May 21, 2014, https://www.bostonglobe.com/magazine/2014/05/21/ways-social-media-can-ruin-your-life/St8vHIdqCLk7eRsvME3k5K/story.html.
[89] Mateescu et. al., *Social Media Surveillance*; Brandon Giggs, *Teen failed for Facebook 'joke' is released*, CNN, Jul. 13, 2013 (discussing a teenager who was arrested after making a "threat" that, when viewed in context, appears to be sarcasm), http://www.cnn.com/2013/07/12/tech/social-media/facebook-jailed-teen/; Ellie Kaufman, *Social Media Surveillance Could have a Devastating Impact on Free Speech. Here's Why.*, MIC, Jan. 19, 2016, https://mic.com/articles/132756/social-media-surveillance-could-have-a-devastating-impact-on-free-speech-here-s-why.
[90] *See, e.g.*, *NAACP v. Button*, 83 S. Ct. 328 (1963); *Citizens United v. Fed. Election Comm'n*, 130 S. Ct. 876 (2010).

sent a letter to Attorney General Jeff Sessions raising concerns about how the federal government and federal law enforcement agencies used technologies that monitored social media.[91] Those Representatives noted how social media was effectively being used to monitor people who were suspected of no wrongdoing in violation of their Fourth Amendment rights stating:

> There is evidence that social media data has been used to monitor protests and activists…An investigator at the Oregon Department of Justice used a service called DigitalStakeout to search Twitter for tweets using the hashtag #BlackLivesMatter. On the basis of his tweets – which included political cartoons and commentary but no indications of criminal activity or violence – the Department's own Director of Civil Rights was deemed a "threat to public safety."[92]

The same concerns are present in CBP's current proposal and these concerns must be addressed before any further steps are taken.

The inclusion of social media information in the CIRS database is often the key that ties together discrete bits of personal data.[93] In the past, the United States has sought to regulate the collection and use of the Social Security Number precisely because of the concern that is leads to government profiling.[94] The availability of the SSN has been shown to contribute to identity theft and financial fraud.[95]

A social media identifier is not private in the sense that it is a secret. But the collection of a social media information by the government does raise privacy concerns because it enables

---

[91] Letter to Jeff Sessions from Keith Ellison et al., May 2, 2017, https://www.documentcloud.org/documents/3696481-House-Democrats-Letter-to-Sessions-re-Social.html.
[92] *Id.*
[93] *Social Security Numbers*, EPIC, https://epic.org/privacy/ssn/.
[94] Testimony of Marc Rotenberg, Computer Professionals for Social Responsibility, "Use of Social Security Number as a National Identifier," Before the Subcomm. on Social Security of the House Comm. on Ways and Means, 102d Cong., 1st Sess. 71 (February 27, 1991). republished Marc Rotenberg, "The Use of the Social Security Number as a National Identifier," *Computers & Society,* vol. 22, nos. 2, 3, 4 (October 1991); Privacy Act of 1974, 5 U.S.C. §552a (2016).
[95] *Identity Theft*, EPIC, https://epic.org/privacy/idtheft/; *Social Security Numbers*, EPIC, https://epic.org/privacy/ssn.

enhanced profiling and tracking of individuals. Furthermore, an individual has no way of knowing who in the government may be tracking them and for how long that surveillance could continue. What is initially presented as a way to facilitate the CBP's identification of threats to national security and public safety can turn into unwarranted, large scale surveillance of innocent people.

V. Conclusion

For the foregoing reasons, the CIRS database is contrary to the core purpose of the federal Privacy Act. Accordingly, the CBP must limit the records contained in the CIRS database and the individuals to whom the records pertain, narrow the scope of its proposed Privacy Act exemptions, and remove the proposed unlawful routine use disclosures from the CIRS system of records.

Additionally, the collecting of social media information undermines First Amendment rights of speech, expression, and association and should be withdrawn. EPIC recommends that any current use of social media analysis by CBP should be reviewed to determine whether it is necessary, whether it undermines First Amendment protected activities, and to determine what safeguards are in place and if the safeguards ensure appropriate oversight and public transparency.

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President and Executive Director

/s/ Jeramie D. Scott
Jeramie D. Scott
EPIC National Security Counsel