Before the

PRIVACY OFFICE
U.S. DEPARTMENT OF HOMELAND SECURITY

Washington, DC 20528

Privacy Act of 1974, Notice of New Privacy Act System of Records, DHS/CBP-024 CBP Intelligence Records System (CIRS) System of Records; Docket Number DHS 2017-0027, FR Doc. 2017-19718 and Privacy Act of 1974, Notice of Proposed Rulemaking: Implementation of Exemptions, DHS/CBP-024 CBP Intelligence Records System (CIRS); Docket Number DHS 2017-0026, FR Doc. 2017-19717	**Comments of The Identity Project (IDP), Restore The Fourth, Inc., Woodhull Freedom Foundation, Defending Rights & Dissent, Government Information Watch, National Coalition Against Censorship (NCAC), FirstAmendment.com, Cyber Privacy Project (CPP), and Government Accountability Project (GAP)**

The Identity Project (IDP)

<https://PapersPlease.org>

October 23, 2017

The undersigned civil liberties and human rights organizations – The Identity Project (IDP), Restore The Fourth, Inc., Woodhull Freedom Foundation, Defending Rights & Dissent, Government Information Watch, National Coalition Against Censorship (NCAC), FirstAmendment.com, Cyber Privacy Project, and Government Accountability Project (GAP) – submit these comments in response to the "Notice of New Privacy Act System of Records, DHS/CBP-024 CBP Intelligence Records System (CIRS)", Docket Number DHS 2017-0027, FR Doc. 2017-19718, 82 *Federal Register* 44198-44203 (September 21, 2017); and the "Notice of Proposed Rulemaking, Privacy Act of 1974: Implementation of Exemptions, DHS/CBP-024 CBP Intelligence Records System (CIRS)", Docket Number DHS 2017-0026, FR Doc. 2017-19717, 82 *Federal Register* 44124-44126 (September 21, 2017).

1. About the commenters

The Identity Project (IDP) provides advice, assistance, publicity, and legal defense to those who find their rights infringed, or their legitimate activities curtailed, by demands for identification, and builds public awareness about the effects of ID requirements on fundamental rights. IDP is a program of the First Amendment Project, a nonprofit organization providing legal and educational resources dedicated to protecting and promoting First Amendment rights.

Restore The Fourth, Inc., is a national, non-partisan civil liberties organization dedicated to robust enforcement of the Fourth Amendment to the United States Constitution. Restore the Fourth believes that everyone is entitled to privacy in their persons, homes, papers, and effects and that modern changes in technology, governance, and law should foster the protection of this right. To advance these principles, Restore The Fourth oversees a network of

local chapters, whose members include lawyers, academics, advocates, and ordinary citizens. Each chapter devises a variety of grassroots activities designed to bolster political recognition of Fourth Amendment rights. On the national level, Restore The Fourth also files amicus briefs in significant Fourth Amendment cases.

Established in February, 2003, **The Woodhull Freedom Foundation** is a 501(c)3 non-profit organization devoted to education and public advocacy in support of the principle that sexual freedom is a fundamental human right. Woodhull works in partnership with activists, advocacy organizations and coalitions across the United States fighting the political, social and economic forces driving and expanding restrictions on our personal autonomy.

Defending Rights & Dissent is a national non-partisan organization that protects the right of political expression to strengthen participatory democracy and to ensure that the promise of the Bill of Rights is fulfilled for everyone.

Government Information Watch is focused on open and accountable government. Our mission is to monitor access to information about government policy, process, and practice and to ensure and preserve open, accountable government through advocacy. In this capacity, we intend to serve as a resource for policymakers, the media, advocacy groups, and the public.

The National Coalition Against Censorship (NCAC) is an alliance of 56 national civil liberties, educational, professional, labor and religious groups. NCAC promotes freedom of thought, inquiry and expression and opposes all forms of censorship.

FirstAmendment.com is a law firm advocating for First Amendment rights.

The Cyber Privacy Project (CPP) is a non-partisan organization focusing on governmental intrusions against Fourth and Fifth Amendment rights of privacy, particularly in

government databanks and national identification schemes for voting, travel, and work, and on medical confidentiality and patient consent.

The Government Accountability Project (GAP) is the nation's leading whistleblower protection and advocacy organization. A non-partisan public-interest group, GAP litigates whistleblower cases, helps expose wrongdoing to the public, and actively promotes government and corporate accountability. Since 1977, GAP has helped over 6,000 whistleblowers.

2. Summary of Objections

As described in the System Of Records Notice (SORN), this system of records would include records of how individuals exercise rights guaranteed by the First Amendment to the U.S. Constitution, in violation of the Privacy Act. This system of records would include records which could be, but would not be, collected directly from the individuals to whom they pertain, in violation of the Privacy Act. This system of records would include records pertaining to categories of individuals not disclosed in the SORN, in violation of the Privacy Act.

The SORN contains materially false claims concerning the status of the rulemaking for Privacy Act exemptions which are directly contradicted by the Notice of Proposed Rulemaking for those exemptions published the same day as the SORN in the *Federal Register*. Because the SORN falsely claims that the Secretary of Homeland Security has exempted this system of records from certain of the requirements of the Privacy Act, when the Secretary has not done so, the SORN is invalid on its face: It fails to provide the public with accurate notice of whether individuals can obtain access to records pertaining to themselves, as required by the Privacy Act. Unless and until a new, valid SORN satisfying the notice requirements of the Privacy Act is duly

promulgated and published in the *Federal Register*, willful maintenance of this system of records would be a criminal offense on the part of the responsible DHS officials or employees.

The false statements in the SORN concerning the status of the rulemaking for Privacy Act exemptions provide *prima facie* evidence of DHS bad faith in conducting this rulemaking. The statement in the SORN that the Secretary has already exempted this system of records from certain provisions of the Privacy Act suggests that the outcome of the exemption rulemaking has already been determined, and that the solicitation and "consideration" of public comments is a sham. Such a decision-making procedure violates the Administrative Procedure Act.

The System of Records Notice and the Notice of Proposed Rulemaking for Privacy Act exemptions should be withdrawn, and any information already collected in categories prohibited by the Privacy Act or beyond the scope of prior System of Records Notices should be expunged.

3. CIRS would include records of how individuals exercise rights guaranteed by the First Amendment to the U.S. Constitution, in violation of the Privacy Act.

According to the SORN for the CBP Intelligence Records System (CIRS), "CIRS records were previously covered by the Automated Targeting System [ATS] SORN and the Analytical Framework for Intelligence [AFI] System SORN."

We maintain the objections we have submitted previously to the DHS concerning the information included in ATS and the operation of this system in violation of the Privacy Act.[1]

1 Comments of The Identity Project and John Gilmore, "Privacy Act of 1974, System of Records Notice (SORN), DHS/CBP-006, Automated Targeting System (ATS)," DHS-2006-0060 (December 4, 2006), <http://hasbrouck.org/IDP/IDP-ATS-comments.pdf>; Supplementary Comments of The Identity Project and John Gilmore, "Privacy Act of 1974, System of Records Notice (SORN), DHS/CBP-006, Automated Targeting System (ATS)," DHS-2006-0060 (December 29, 2006), <https://hasbrouck.org/IDP/IDP-ATS-comments2.pdf>; Comments of The Identity Project and John Gilmore, "Notice of Proposed Rulemaking, Privacy Act of 1974, Implementation of Exemptions, Automated Targeting System," DHS-2007-0043 (September 5, 2007), <https://hasbrouck.org/IDP/IDP-ATS-comments3.pdf>.

We also believe that AFI violates the Privacy Act and the First Amendment in similar ways.[2]

While we reiterate those objections, we address these comments to the additional categories of information, sources, and individuals covered by the SORN for CIRS which were not mentioned in any of the the previous SORNs for ATS or AFI.

According to the SORN, the categories of records in CIRS would include "Articles, public-source data (including information from social media), and other published information on individuals and events of interest to CBP." Additional record source categories would include "private sector entities and organizations, individuals, commercial data providers, and public sources such as social media, news media outlets, and the Internet."

The Privacy Act of 1974, 5 U.S.C. 552a(e)(7), requires that:

> "Each agency that maintains a system of records shall --... maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."

It should go without saying that records of "information from social media" obtained form "social media, news media outlets, and the Internet" are records of how individuals exercise rights guaranteed by the First Amendment, including the right to freedom of speech, the right to freedom of the press, and the right of the people peaceably to assemble.

Social media is speech, whether in words or music or photos or videos. Records of our posts, comments, photos, videos, and other things we say on social media are, *per se*, records of how we exercise our First Amendment right to freedom of speech.

---

2 See The Identity Project, "'AFI' is the latest DHS name for 'extreme vetting'", December 21, 2016, <https://papersplease.org/wp/2016/12/21/afi-is-the-latest-dhs-name-for-extreme-vetting/>, and The Identity Project, "Palantir, Peter Thiel, Big Data, and the DHS" (March 15, 2017), <https://papersplease.org/wp/2017/03/15/palantir-peter-thiel-big-data-and-the-dhs/>.

Social media platforms and news media outlets are publishing platforms. Records of what we post, share, upload, or otherwise publish on social media platforms or news media outlets are, *per se*, records of how we exercise our First Amendment right to freedom of the press.

Social media is, by definition, social. People don't participate in social media as individuals, but in association with others. Social media network maps, lists of "friends" or "followers", or records of who "likes" or "shares" or comments on our posts, who we associate with in other ways on social media, or how we do so are, *per se*, records of how we exercise our First Amendment right to assemble online – the social media equivalent of a mail cover, a telephone call log, or a list of attendees and speakers at an in-person political meeting.

The right to assemble in cyberspace is, of course, especially critical to the right to assemble across U.S. and other national borders and by citizens and residents of different countries, for whom visa and immigration rules and, in some cases, fear of government persecution or other hazards may make in-person assemblies difficult, dangerous, or impossible.

The Privacy Act permits the maintenance by a Federal agency of records such as these of how we exercise rights guaranteed by the First Amendment only if it is: (a) expressly authorized by statute, (b) expressly authorized by the individual about whom the record is maintained, or (c) pertinent to and within the scope of an authorized law enforcement activity.

The proposed maintenance of social media, news media, and Internet records in CIRS does not satisfy any of these three conditions.

First, there is no explicit authorization in any Federal statute for any surveillance, recording, or maintenance of records of social media activities. None of the statutes cited as authority for the maintenance of CIRS contains any explicit mention of social media, much less

explicit authorization for the maintenance of these records. It is irrelevant whether authorization might arguably be implicit in some general authority claimed by CBP for monitoring of all aspects of the lives and activities of non-U.S. persons, international travelers, and U.S. persons who associate with them. The Privacy Act requires express statutory authorization.

Second, it is patently obvious that the maintenance of these records has not been "expressly authorized by ... the individuals about whom these records are maintained".

CBP has never asked for permission to "friend" or "follow" us on social media or to record what we say and who we associate with on social media in its permanent files about us – as would be required by this provision of the Privacy Act for this CBP activity to be permissible.

Implicit authorization does not satisfy the Privacy Act. Explicit authorization from those about whom records are kept, which CBP has neither sought nor obtained, is required.

The lack of even implicit statutory authorization or authorization from data subjects is especially clear with respect to U.S. citizens who associate with foreigners on social media.

Social media platforms have global reach. We do not normally know, and may not care, whether people we associate with on social media are U.S. citizens, permanent U.S. residents, holders of visas for entry to the U.S., foreign citizens and residents, or stateless persons.

"Relationship status" is a standard element of a Facebook profile, but "U.S. citizenship or immigration status" is not a typical or required element of a social media profile.

But CBP does not ask U.S. citizens, before we friend or follow a foreigner on social media, whether we are aware that this person is not a U.S. person, and that our association with this person on social media will be subject to recording in permanent CBP files.

Similarly, while the categories of individuals covered by the system would be extended to include "Individuals identified in public news reports", CBP cannot possibly pretend to have obtained the consent of individuals mentioned in news reports for CBP to retain this information.

This is exactly the sort of activity that the Privacy Act was enacted to prohibit, following disclosures that the FBI under J. Edgar Hoover had compiled dossiers about individuals' protected First Amendment activities comprised of this sort of "public source" information.

Third, the maintenance of these social media records is not, “pertinent to and within the scope of an authorized law enforcement activity.”

With respect to whether this record-keeping is “pertinent to … an authorized law enforcement activity,” whether any proposed use of this sort of information about pure speech and assembly is authorized by law or by the U.S. Constitution would be subject to strict scrutiny.

The SORN does not explain how or why the DHS believes that evidence about who U.S. persons associate with on social media, especially if they are not suspected of any crime, is pertinent to any authorized law enforcement activity.

Our system of justice is founded on the notions of individual responsibility and of judgment for our own, and only our own, actions. Absent evidence of criminal conspiracy, collective judgment or guilt by association is anathema to our legal principles. Who we associate with is not, in most circumstances, relevant to whether we have committed a crime.

Travel by U.S. citizens, including travel across U.S. borders, and association with non-U.S. persons, are acts by which we exercise of our right to assemble. The exercise of First Amendment rights cannot Constitutionally be treated as *per se* suspicious.

Even if CBP were to establish that some of this record-keeping is, in some tenuous way, "pertinent to" some vaguely-inferred authority for social media surveillance for general law enforcement purposes – which CBP has not done, and which we do not believe it can do – the Privacy Act would also require that it be "within the scope" of that authorized purpose.

The scope of the record-keeping described by the SORN is essentially unlimited, and extends to essentially every individual in the world who interacts with other people on social media, including most U.S. citizens, or who is mentioned in any news report or on the Internet.

The SORN does not define who would be considered "associates" of an individual social media user, or limit the number of degrees of separation at which friends-of-friends or friends-of-friends-of-friends would be deemed "associates". Many U.S. persons have some non-U.S. persons among their direct social media associates as friends, followers, commenters, etc. – often without knowing that they are not U.S. persons. Almost all social media users anywhere in the world, including U.S. persons, have at least some non-U.S. persons within a few degrees of indirect "association" on social media.

U.S. persons do not live in splendid isolation. We are all associates of non-U.S. persons.

Pursuant to the SORN, this System of Records would become a general system of dragnet surveillance of social media activities by all individuals worldwide regardless of citizenship. Such dragnet social media surveillance of U.S. persons, not based on warrants or probable cause, is not within the scope of any authorized CBP law enforcement activity.

CBP may claim that it will, in its discretion, exercise self-restraint and conduct only limited social media, news media, and/or Internet surveillance and record-keeping. But the

SORN, which must be assessed on its own terms, contains no such limits, and no such limitation would be feasible. The SORN gives notice of practices which will violate the Privacy Act.

We doubt that social media surveillance and "public source" news media and Internet monitoring can be conducted by CBP in such a limited way that it would be consistent with the Privacy Act and the U.S. Constitution. But if CBP believes that is can be so limited as to be legal, CBP needs to publish a new SORN limited to lawful records before it starts operating such a system of records.

The possibility that the exercise on social media by any U.S. or foreign person of her rights to freedom of speech, freedom of the press, and freedom to assemble might be monitored and retained in a DHS system of records, and be “shared” by the DHS with third parties including other U.S. government agencies and other governments around the world, is already exerting a profound chilling effect on the exercise of First Amendment rights by individuals in the U.S. and around the world.

4. CIRS would include records which could be, but would not be, collected directly from the individuals to whom they pertain, in violation of the Privacy Act.

The Privacy Act of 1974, 5 U.S.C. 552a(e)(2), requires that:

> “Each agency that maintains a system of records shall --... collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual’s rights, benefits, and privileges under Federal programs.”

If for some reason CBP wants to know what an individual has said or published on social media or otherwise on the Internet, and that information is pertinent to some authorized CBP

function (which would presumably mean that it could lawfully be used as part of the basis for some adverse determination), CBP can ask that individual to provide that information directly.

The SORN gives no argument as to why this would not be practicable.

5. CIRS would include records pertaining to categories of individuals not disclosed in the SORN, in violation of the Privacy Act.

CBP has no way to know, when information about social media activities, public news reports, or information from other Internet sources is collected and recorded, whether the individuals to which it pertains are U.S. persons. In light of the inclusion of social media information, news reports, other Internet sources, and associations in this system of records, the "Categories of Individuals Covered by the System" must be amended, and a new SORN published in the *Federal Register*, giving the public fair warning that all social media users worldwide, regardless of citizenship, are potentially subject to having records of our activities included in this System of Records.

6. The SORN contains materially false claims concerning the status of the rulemaking for Privacy Act exemptions which are directly contradicted by the Notice of Proposed Rulemaking for those exemptions.

The description of "Record Access Procedures" in the SORN begins with the following false claim:

> The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and the Judicial Redress Act if applicable, because it is a law enforcement system.

Exemption of a System of Records from these provisions of the Privacy Act is permitted only in accordance with 5 U.S.C. 552a(j) and 552a(k), which provide that:

> The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency..."

If the Secretary of Homeland Security had purported to exempt this System of Records from any of the requirements of the Privacy Act – as falsely claimed in the SORN – without complying with the notice and other requirements of agency rulemaking, that action would be invalid as failing to comply with the Privacy Act and the Administrative Procedure Act.

In fact, the Secretary of Homeland Security has not taken such an action. On the contrary, the DHS has, in the same edition of the *Federal Register* as the SORN, promulgated a Notice of *Proposed* Rulemaking for Privacy Act exemption, by which NPRM the DHS gives notice and solicits comments from the public, to be considered before a decision is made, of proposed rules to exempt this System of Records from some of the requirements of the Privacy Act.

By misstating the status of the exemption rulemaking, the SORN gives false information about record access procedures – a required element of a SORN – and is invalid on its face.

At a minimum, a new SORN must be promulgated, accurately stating that the DHS has proposed to exempt this System of Records from certain specified requirements of the Privacy Act, but has not yet finalized any rules to do so, before this System of Records can be created.

Whatever the merits of the proposed exemptions, the fact that the DHS stated in the SORN that the Secretary of Homeland Security had already made her decision to exempt this System of Records from these requirements provides *prima facie* evidence of DHS bad faith in conducting this rulemaking. This statement suggests that the outcome of the exemption

rulemaking has already been determined, and that the solicitation and "consideration" of public comments is a sham. Such a process violates the Administrative Procedure Act.

Pursuant to the Privacy Act and the Administrative Procedure Act, CIRS will not be exempt from any of the requirements of the Privacy Act unless and until a final rule is promulgated in accordance with all of the required procedures for rulemaking.

We find this false and misleading SORN especially disturbing because this is not the first time that the DHS has promulgated a SORN for some of these same records that was facially invalid because of false claims as to the status of rulemaking for Privacy Act exemptions.

As noted above, DHS says that some of the records in CIRS were previously considered part of ATS. ATS contains records dating to at least 1992, but the first SORN for ATS was published in 2006.[3] In that SORN, DHS stated that, "DHS intends to … if warranted, issue a new set of exemptions specific to ATS within ninety (90) days of the publication of this notice." But the DHS did not do so: no NPRM or final rule for exemptions was promulgated.

In 2007, DHS promulgated a revised SORN for ATS, in which the DHS stated that, "Pursuant to 6 CFR Part 5, Appendix C, certain records and information in this system are exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (e)(5), and (8); (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k)(2))."[4]

In fact, as of the 2007 date of that SORN, 6 CFR Part 5, Appendix C, contained no rules exempting ATS. But the same day that this facially invalid SORN falsely claiming that

3 "Notice of Privacy Act System of Records, Automated Targeting System (ATS)", DHS-2006-0060, 71 *Federal Register* 64543-64546 (November 2, 2006).

4 "Notice of Privacy Act System of Records, Automated Targeting System (ATS)", DHS-2007-0042, 72 *Federal Register* 43650-43656 (August 6, 2007).

exemptions for ATS were already part of the CFR was published, the DHS promulgated a Notice of Proposed Rulemaking soliciting public comment on possible exemptions for ATS.[5]

The DHS did not promulgate any final rule for Privacy Act exemptions for ATS until 2010.[6] Throughout the intervening years, maintenance of the ATS System of Records without a valid SORN giving accurate notice of the record access procedures was a criminal offense – as operation of CIRS will be unless and until either a new and valid SORN (properly stating that no exemption rules have yet been finalized) is promulgated, or the DHS completes a proper notice-and-comment rulemaking (including genuine consideration of public comments).

The SORN and the NPRM for Privacy Act exemptions should be withdrawn, any information already collected should be expunged, and any CBP or DHS officials responsible for willfully operating a system of records without a valid SORN should be prosecuted.

5 "Notice of Proposed Rulemaking: Implementation of Exemptions, Automated Targeting System", Docket Number 2007-0043, 72 Federal Register 43567-43569 (August 6, 2007).

6 "Final Rule: Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Customs and Border Protection-006 Automated Targeting System of Records", DHS-2009-0055, 75 *Federal Register* 5487-5491 (February 3, 2010).

Respectfully submitted,

The Identity Project (IDP)

<https://PapersPlease.org>

A project of the First Amendment Project

1736 Franklin St., 9th Floor

Oakland, CA 94612

/s/

Edward Hasbrouck,

Consultant to IDP on travel-related issues

Restore The Fourth, Inc.

<https://www.restorethe4th.com>

Woodhull Freedom Foundation

<https://www.woodhullfoundation.org>

1601 18th Street, NW #104

Washington, DC 20009

Defending Rights & Dissent

<https://rightsanddissent.org>

Government Information Watch

<http://govinfowatch.net>

National Coalition Against Censorship (NCAC)

<http://ncac.org>

19 Fulton St., Suite 407

New York, NY 10038

FirstAmendment.com

<http://www.firstamendment.com>

195 W. Pine Ave.

Longwood, FL 32750

Cyber Privacy Project (CPP)

<http://www.cyberprivacyproject.org>

Government Accountability Project (GAP)

<https://www.whistleblower.org>

Louis Clark, CEO

1612 K. St. NW, Suite #1100

Washington DC, 20006