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/ALL-041 External Biometric Records (EBR) System of Records; Docket Number DHS 2017-0039, FR Doc. 2018-08453 and Privacy Act of 1974, Notice of Proposed Rulemaking: Implementation of Exemptions, DHS/ALL-041 External Biometric Records (EBR) System of Records; Docket Number DHS 2017-0040, FR Doc. 2018-08454	**COMMENTS OF THE IDENTITY PROJECT (IDP), GOVERNMENT INFORMATION WATCH, CYBER PRIVACY PROJECT (CPP), RESTORE THE FOURTH, INC., AND NATIONAL IMMIGRATION LAW CENTER (NILC)**

The Identity Project (IDP)

<https://PapersPlease.org>

May 24, 2018

The undersigned civil liberties and human rights organizations – the Identity Project (IDP), Government Information Watch, Cyber Privacy Project (CPP), Restore the Fourth, Inc., and National Immigration Law Center (NILC) – submit these comments in response to the "Notice of New Privacy Act System of Records, DHS/ALL-041 External Biometric Records (EBR) System of Records", Docket Number DHS 2017-0039, FR Doc. 2018-08453, 83 *Federal Register* 17829-17833 (April 24, 2018); and the "Notice of Proposed Rulemaking, Privacy Act of 1974: Implementation of Exemptions, DHS/ALL-041 External Biometric Records (EBR) System of Records", Docket Number DHS 2017-0040, FR Doc. 2018-08454, 83 *Federal Register* 17766-17768 (April 24, 2018).

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.

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 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.

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.

The National Immigration Law Center (NILC), established in 1979, is one of the leading organizations in the U.S. exclusively dedicated to defending and advancing the rights and opportunities of low-income immigrants and their families. Our mission is grounded in the belief that every American — and aspiring American — should have the opportunity to fulfill their full potential, regardless of where they were born or how much money they have.

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, without explicit statutory authorization for their collection, 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 categories of records not listed in the “Categories of Records in the System” section of 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 (NPRM) 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.

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 SORN and the NPRM 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. EBR 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 External Biometric Records (EBR) System of Records, "Information collected by a *non-DHS entity* and and maintained in this system includes:… location and circumstance of each instance resulting in biometric collection."

Additionally, according to the section of the SORN concerning “Policies and Practices for Retention and Disposal of Records,” these records will be used to generate derivative “records related to the analysis of relationship patterns among individuals and organizations … including possible… non-obvious relationships.”

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.”

Records of and related to individuals’ movements, locations, and patterns of associations between individuals and organizations are records of how individuals exercise rights guaranteed by the First Amendment, including the right of the people peaceably to assemble.

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 location and incident logs pertaining to the collection of biometric data (for example, logs of the places and times when a facial image determined by a DHS or third-party algorithm to be that of a specific individual was captured by a third-party surveillance camera) do not satisfy any of these three conditions.

First, there is no explicit authorization in any Federal statute for biometric-based logging of locations, movements, and associations between U.S. persons. None of the statutes cited as authority for the maintenance of EBR contains any explicit mention of location or movement logs or biometric-based attempts to map patterns of associations and organizations. It is irrelevant whether authorization might arguably be implicit in some general authority claimed by DHS. The Privacy Act requires express statutory authorization, and there is no such authorization for comprehensive biometric-based monitoring of U.S. citizens' movements and associations.

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".

The DHS has never asked for permission to track and log our locations, movements, organizations, associations, and when, where, and with whom we assemble – as would be required by this provision of the Privacy Act for this DHS activity to be permissible.

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

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 including third-party "derogatory information."

Third, the maintenance of these location, movement, association, and organization 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 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, movement, and association 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 the DHS were to establish that some of this record-keeping is "pertinent to" some inferred authority for surveillance of our locations, movements, and association for general law enforcement purposes – which the DHS 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 all "individuals whose biometric and associated biographic information are collected by non-DHS entities for the following DHS purposes...." Not all of the purposes listed are limited to, or within the scope of, law enforcement activities.

The SORN gives notice of practices which will violate the Privacy Act. We doubt that location and movement logging and mapping of associations and organizations can be conducted by the DHS in such a limited way that these these activities would be consistent with the Privacy Act and the U.S. Constitution. But if the DHS believes that these activities can be so limited as to be legal, the DHS needs to publish a new SORN limited to lawful records before it starts operating such a system of records.

4. EBR 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), provides 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."

According to the SORN, all of the records in EBR are collected by non-DHS entities. None of them are collected directly by any DHS component from the subject individuals. But in this NPRM, the DHS proposes to exempt EBR records from this provision of the Privacy Act.

In other words, the DHS wants to use biometric identifiers such as facial recognition to track and log our locations, movements, associations, and organizations, but does not want us to be aware of, or able to opt out of, this pervasive government surveillance.

The SORN makes clear that the purpose of collecting and maintaining EBR records is to use them as part of the basis for making of a variety of potentially adverse determinations about individuals' rights, benefits, and privileges under Federal programs.

As its sole justification for exempting these records from this provision of the Privacy Act, the NPRM for Privacy Act exemptions claims that, "requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities." But this rationale would apply only to records pertaining to the subjects of law enforcement investigations. EBR would contain records about many other individuals.

At a minimum, the proposed exemption rule should be amended to exempt only records concerning the subjects of law enforcement investigations based on reasonable suspicion.

Normally, an individual asked to identify herself to the DHS or any government agency, even the subject of a Terry stop, has the Fifth Amendment right to stand mute.

If the DHS wants to collect biometric information about other individuals, or information about their locations, movements, associations, or organizations, it can ask them to provide that information directly – and they can choose to say, "No."

5. EBR would include categories of records not listed in the "Categories of Records in the System" section of the SORN, in violation of the Privacy Act.

The SORN contains clear internal evidence that EBR would include categories of records not listed in the "Categories of Records in the System" section of the SORN.

The section of the SORN concerning "Policies and Practices for Retention and Disposal of Records" refers to the retention of, "Records related to the analysis of relationship patterns among individuals and organizations… including possible… non-obvious relationships."

But these records of "relationship patterns among individuals and organizations" – records of pure First Amendment protected acts of assembly – are not mentioned in the "Categories of Records in the System" section of the SORN.

The "Categories of Records in the System" must be amended, and a new SORN published in the *Federal Register*, giving the public fair warning of the proposal to collect and maintain (secret) files concerning our associations and organizations.

Unless and until such a new SORN is promulgated, the operation of a system of records containing records in categories not disclosed in the SORN, including records of associations and organizations, would be a criminal offense on the part of the responsible Department officials.

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 section of the SORN concerning "Record Access Procedures" 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 consequently 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 as follows:

> 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 exemptions, 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, EBR 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.

Maintenance of the EBR System of Records without a valid SORN giving accurate notice of the record access procedures will be a criminal offense on the part of the responsible DHS officials 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 exemption 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 DHS officials responsible for willfully operating a system of records without a valid SORN should be prosecuted.

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

Government Information Watch

<http://govinfowatch.net>

Cyber Privacy Project (CPP)

<http://www.cyberprivacyproject.org>

Restore The Fourth, Inc.

<https://www.restorethe4th.com>

National Immigration Law Center

<https://www.nilc.org>