Comments of World Privacy Forum

to

Department of Homeland Security

regarding

Proposal to Establish a New DHS System of Records, Department of Homeland Security/ALL-041 External Biometric Records (EBR) System of Records

and

Proposal to Exempt New DHS External Biometric Records (EBR) from Key Provisions of the Privacy Act of 1974

Docket Nos: DHS-2017-0040 and DHS-2017-0039

Via Federal Rulemaking Portal, https://www.regulations.gov/

Philip S. Kaplan,
Chief Privacy Officer
Privacy Office
Department of Homeland Security
Washington, DC 20528

May 24, 2018

The World Privacy Forum appreciates the opportunity to comment on the important System of Records Notice and the concurrently published Notice of Proposed Rulemaking at 83 Federal Register 17829 (April 24, 2018) and 83 Federal Register 17766 (April 24, 2018). The notices pertain to the US Department of Homeland Security's External Biometric Records database. The notices are available at

https://www.gpo.gov/fdsys/pkg/FR-2018-04-24/html/2018-08453.htm and https://www.gpo.gov/fdsys/pkg/FR-2018-04-24/html/2018-08454.htm.

The World Privacy Forum is a non-profit public interest research group that focuses on data privacy issues, including those relating to technology, health, biometrics, and other topics. Our research, testimony, consumer education, and other materials can be found on our webpage, www.worldprivacyforum.org.

I. Introduction and background of comments

The System of Records Notice (SORN) discussed in this comment describes the External Biometrics Records database (EBR database). The Notice of Proposed Rulemaking (NPRM) we are also commenting about was published concurrently, and provides sweeping exemptions for the EBR database from requirements of the Privacy Act of 1974.

In overview, the SORN and NPRM pertain to DHS's External Biometric Records database, described as a system of records that comprises a large and important biometric and demographic database, drawn from foreign and domestic sources. In addition to traditional biometric and demographic data, the EBR database will also include diverse commentary and also derivative analysis, which will not have been collected directly from individuals. The database will contain data of varying degrees of accuracy and quality. The rights of access, accuracy, and many other rights typically associated with data held by the US government do not apply to the EBR database due to the exemptions DHS has granted it in the NPRM. Additionally, a number of Routine Uses have been proposed, some of which are problematic.

According to the SORN, external biometric data is already being collected by entities that are not subject to the Privacy Act of 1974. From the notice:

> External information is collected by non-DHS entities, including the Department of Defense (DoD), the Department of Justice (DOJ), State and local law enforcement authorities, or foreign governments.

The notice goes on to describe the nature and type of biometric information being collected:

> External information shared with DHS includes biometric (*e.g.,* latent fingerprints) and associated biographic information that may be used by DHS

The notice states that the uses of the collected data will be extremely broad, and are listed as follows:

> ...information ...may be used by DHS for the following purposes: Law enforcement; national security; immigration screening; border enforcement; intelligence; national defense; and background investigations relating to national

> security positions, credentialing, and certain positions of public trust, consistent with applicable DHS authorities.
> DHS also maintains this information to support its information sharing agreements and arrangements with foreign partners to: Prevent travelers from assuming different identities to fraudulently gain admission or immigration benefits; identify individuals who seek to enter the United States for unauthorized purposes; identify those who have committed serious crimes or violated immigration law; enable informed decisions on visas, admissibility, or other immigration benefits. Such sharing augments the law enforcement and border control efforts of both the United States and its partners. Additionally, DHS is using this information in concert with external partners to facilitate the screening of refugees in an effort to combat terrorist travel consistent with DHS's and Components' authorities.
> Consistent with DHS's mission, information covered by DHS/ALL-041 EBR may be shared with DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS may share information with appropriate Federal, State, local, tribal, territorial, foreign, or international government agencies from the providing external entity, consistent with any applicable laws, rules, regulations, and information sharing and access agreements or arrangements. DHS may share biometric and associated biographic information as permitted pursuant to an applicable Privacy Act authorized disclosure, including routine uses set forth in this SORN. Additionally, DHS is issuing a NPRM to exempt this system of records from certain provisions of the Privacy Act elsewhere in the Federal Register. This newly established system will be included in DHS's inventory of record systems.

We specifically note that DHS has exempted the EBR database from the requirements of the Privacy Act regarding **accuracy**, which is remarkable for a system of such high sensitivity and for a system that will have a high impact on individuals' civil liberties.

We have significant concerns about this proposed System of Records and how DHS is proposing to both exempt it from multiple provisions of the Privacy Act, and administer it procedurally. In the comments below, we discuss the details of our concerns and we both suggest and request solutions.

II. Specific Comments

A. Problematic Routine Uses

We are concerned with a number of the Routine Uses proposed in the system of records notice.

Routine use E regarding data breach is overbroad and non-specific. We request that the Routine Use E be amended to require someone at a high level (GS-15 or above), CPO, CTO, Agency Head or designee, or someone senior to make decisions regarding data

breach activities.

Routine use I is arguably illegal. (b)(7) provides a method for making disclosures to other law enforcement agencies. Those disclosures are excessively broad. Writing a RU to evade the statutory standard in (b)(7) violates the requirement that disclosures be compatible with the purpose for which the records were collected. Helping any agency around the world enforce any law (without restriction) has nothing to do with the reason DHS collected the information. We do not support this Routine Use and request it be removed.

Routine use L has some problems that can be remedied. First, consent should be sought from the individual if possible, and it should be sought first. Even someone who is incapacitated physically could give or withhold consent in many circumstances. Further, the Privacy Act doesn't cover people who are deceased, so the reference to deceased people in Routine use L is incorrect and should be removed.

Routine use M is unrestricted as it does not specify what kind of technology is being tested, and there is nothing that offers protection to individuals whose information is disclosed. We request that the Routine use M be amended to state that disclosures are allowed only if the recipient agrees in writing not to use any information disclosed under the RU against the data subject in any criminal or civil proceeding. We support the requirement for approval of the CPO, and we recommend that this procedural step is included in other Routine Uses, such as Routine Use N.

Routine use N, in the context of a biometrics database, poses major challenges. It is helpful that the CPO must approve activities. But it is hard to imagine when it would be appropriate to **publicly** release most biometrics. We wonder: when would it ever be appropriate to release DNA publicly? Other than a photo and physical description in limited circumstances, we see this routine use as overbroad. Even then, since all the information comes from external sources, it would be more appropriate for the source to either be consulted first or for the original source to make the disclosure under its own authority. It is possible that DHS could make a disclosure that the source could not make itself, creating all kinds of regulatory and potential cross-jurisdictional challenges. Think about a European resident whose DNA was released by DHS publicly under Routine Use N. We predict that this would be a very challenging circumstance, particularly if there was an error involved. We request that this routine use be substantively narrowed, or at the very least that the DNA aspect be dropped entirely.

B. Quality, accuracy and continuity of external information collected

The World Privacy Forum is concerned about the quality of the biometric and demographic and other data that is received, categorized, maintained, and then disseminated from varying sources for the EBR database.

The exemption of this system of records from the accuracy requirements of the Privacy Act is a mistake because inaccuracies can and will have substantial deleterious impacts

on data subjects. As has been robustly documented, data collected at the border, including border data collected via mobile units, including through mobile biometric and demographic collection technologies, as well as data collected by foreign governments and commercial entities, can contain a high number of errors. This is problematic, because errors entered into the ERB database could (and we predict will) cause erroneous deportations or erroneous criminal charges, and meanwhile, the errors are challenging (or impossible) for the data subject to access or correct. The Judicial Redress Act will not cover all individuals from all jurisdictions, nor will it cover the entirety of the data corrections that will need to be made.

We urge DHS to adopt a process to detect, correct, and fully address the errors in the ERB database, even if the Privacy Act requirements continue to be exempted. Exemptions will not solve the problems that inaccurate data create. We discuss this more in C, below.

C. Transparency of external information collected: Request for publication of database error rates and procedures to correct errors

We understand that due to the nature of the EBR database, in that it is related to law enforcement activities, and in that broad exemptions are being claimed for the database, that data will be extremely difficult for individual data subjects to request and see.

We therefore request and urge that DHS put in place a significant process to detect, correct, and fully address the errors in this system of records. We promise that this system of records will contain errors; it is necessary that the system is accurate in order to be both fair and effective.

Further, we request that DHS publish an annual report describing the error rate of this system, and describe the procedures the agency has put in place to reduce the error rate, and describe, from year to year, changes in the error rate. This is an important oversight and transparency mechanism for the public.

If DHS is going to create this biometric database from multiple sources, including sources that are foreign and/or commercial, it is absolutely essential that the public understand and are informed of the quality of the database being used to make decisions that could impact their lives in meaningful ways. And it is important that DHS is auditing and accounting for errors.

D. Voluntariness of external information collected and direct or indirect collection

The situations under which the data in the biometric and demographic databases are collected will be diverse regarding consent, knowledge, and voluntariness of the data subject. We request that the system of records makes notation of the manner in which the data was collected, whether it was a direct collection from the individual, and whether it was done with the knowledge of the individual. We understand from the SORN that the

location and circumstance of the biometric collection will be noted. The addition of voluntariness and direct or indirect collection would be helpful.

Certain classes and types of biometrics can be collected without the knowledge or consent of the individual. There are many questions about this type of indirect or passive collection, particularly if the data has been collected in a commercial setting. For example, facial biometrics can be collected in many public areas without an individual's knowledge or consent. As biometrics technologies mature, it is likely that it will become increasingly important to note the manner in which the biometric data was collected, and whether it was done with the knowledge of the individual.

E. Categories and types of biometric information collected and source of biometric collection

The SORN did not indicate specific categories or types of biometrics to be collected, nor the sourcing of the biometric data. We request the DHS remedy this oversight by including with specificity the biometric data that will be included in this database, and specify the sources of the biometric data.

We are assuming that the biometrics that are collected will include multi-modal biometrics encompassing facial, gait, and all other biometrics, including fingerprint, iris print, and behavioral biometrics to name a few.

We have many questions about what biometrics will be included, and what the sources for the biometrics will be.

- Will the EBR database include DNA?
- Will the EBR database include biometric data sourced from commercial entities?
- Will the EBR database include biometric data sourced from, for example, retail businesses?
- Will the EBR database include biometric and DNA data from consumer genealogical databases?
- Will the EBR database include biometric and DNA data from medical records?

The World Privacy Forum has deep concerns about governmental use of biometrics collected from commercial settings, medical settings, or from cameras owned or operated by commercial entities. There can be substantive differences in quality, to begin with, among many other issues relating to fairness. We are particularly interested to know whether DNA will be collected in the EBR database, particularly since DHS has stated in Routine Use N that DHS can publicly release biometric data, which at this time appears to include DNA unless it is specifically omitted.

F. Demographic data fields and third party data sources

The SORN does not adequately specify what demographic information is going to be included in the EBR database. This needs to be corrected. We request that the precise demographic information that is to be included in the EBR is listed in the SORN. If DHS believes this is a security risk, we then request that the categories of information be listed.

We also request that if any third party data is used to augment the biometric and demographic data, for example, data purchased from a data broker, that this data will be marked as purchased or 3rd party data.

Data broker data is subject to unknown error rates, and unless and until the error rates of third party data are precisely and unambiguously proven to DHS, then that data should be quarantined until it is proven to be correct through data from the US government and/ or data that has been vetted and has a known, acceptably low error rate.

G. Created and derived data in the EBR database

DHS noted that records in the EBR database will include *created or derived data*, that is, records derived from analytical and predictive processes. The SORN states that the EBR database will include records ....

> related to the analysis of relationship patterns among individuals and organization that are indicative of violations of the customs and immigration laws including possible terrorist threats from non-obvious relationships and specific leads and law enforcement intelligence for active and new investigations.

The World Privacy Forum spent several years researching predictive analytics. We produced an extensively researched report, *The Scoring of America*, available at https://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/, which details the numerous flaws and loopholes inherent in analytical systems of the type the EBR database is using. Predictive algorithms, even those that are well-understood and stable, are subject to errors and bias based on the input data, as well as pathologies arising from the algorithms used in the process. Add to this process additional error arising from input error, and the potential for error is magnified.

Because of these risks, we are proposing that DHS install extremely robust procedures to address problems related to predictive policing tools.

H. Audit and review procedures for collection, maintenance, categorization and analysis, and dissemination of data

It is urgent the DHS put in place extensive and continuous audit and review procedures regarding:

- The collection,
- maintenance,

- categorization,
- analysis,
- and
- dissemination of the External Biometric Records data.

Due to the Privacy Act exemptions the DHS is granting to the EBR database, this database could turn into a large pool of data with a high error rate, which could become a root cause of unfairness and harm for individuals living within the US borders, including US citizens. DHS needs to address these problems now, not later.

Further, DHS needs to abide by a robust code of ethics in regards to everything it does with and around the EBR, and require those whom use or access the data to do so as well. The FBI has a robust Code of Ethics that is publicly available. The DHS may have a similar code, if so, we are unaware of it. We propose that something like the FBI Code of Ethics (https://vault.fbi.gov/fbi-ethics-and-integrity-program-policy-guide/FBI%20Ethics%20and%20Integrity%20Program%20Policy%20Directive%20and%20Policy%20Guide%200754DPG%20Part%2001%20of%2001/view) or a similar robust code of ethics is required for all entities accessing or using the data in the EBR database.

While ensuring ethical standards may seem an unusual request to be made in a public comment regarding a DHS database, this database is of particular interest to all in the US, and has the potential for significant enough abuse and impact that it warrants the application of both legal and ethical protections. In the concurrent Notice of Proposed Rulemaking regarding the installation of the Privacy Act exemptions, DHS stated that the exemptions could be waived on a case by case basis:

> In appropriate circumstances, when compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system and the overall law enforcement process, the applicable exemptions may be waived on a case by case basis.

It is positive that the exemptions can be waived. But the language is unspecific, and the rest of the NPRM does not satisfy what is needed in terms of meaningful rules of the road for exactly how this would be done. It leaves a lot of questions. In order to reduce uncertainty and to ensure consistent, fair results, there needs to be specific, detailed procedural guidance as to when the exemptions can or should be waived, and ethical guidance that makes it clear how employees and others need to approach serious problems of the type that will arise from database errors.

To begin to address these practical questions, we request that DHS create a meaningful roster of exemplar scenarios to illustrate how waiving exemptions would work in real-world scenarios, and designate formal or informal rules to handle the scenarios, with the idea that these rules would be in place to assist DHS employees or others in the field who have to make "where the rubber meets the road" decisions about waiving exemptions.

III. Conclusion

It is a poor outcome that the DHS has decided to give the External Biometric Records database broad exemptions from the protections of the Privacy Act of 1974, and granted such broad Routine Uses, including the position that DHS retains the right to publicly disclose database contents, including DNA. We again urge the DHS to reconsider its position on the public disclosure of DNA. We urge this change in order to facilitate the right data used properly in the right circumstances. It is about getting a good outcome for all, and the right and correct outcome, one which can be trusted.

The EBR database introduces meaningful problems with accuracy, and the legal and ethical complications of relying upon and using data known to have varying degrees of accuracy, including unconsented data. This is not the first time DHS will have to deal with this problem, but it is an important instance. Solutions to these problems exist, but will require meaningful procedural protections to be put in place, sooner, rather than later. We urge DHS to undertake this work. If it is helpful, we stand ready to answer questions.

Respectfully submitted,

Pam Dixon
Executive Director
World Privacy Forum
www.worldprivacyforum.org
+1 760-470-2000