ELECTRONIC FRONTIER FOUNDATION

Comments of the Electronic Frontier Foundation

Regarding

Department of Homeland Security

Proposal to Establish a New DHS System of Records Titled, "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

DHS-2017-0039

May 24, 2018

May 24, 2018

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

Comments on Notice of a New System of Records: Department of Homeland Security/ All-041 External Biometric Records (EBR) System of Records & Proposed Privacy Act Exemptions

Docket Nos.: DHS-2017-0039 / DHS-2017-0040

The Electronic Frontier Foundation (EFF) submits the following comments in response to DHS's proposal to exempt its External Biometric Records (EBR) database from certain provisions of the Privacy Act of 1974, as well as its proposal to replace the System of Records Notice (SORN) for DHS/US-VISIT-001 DHS Automated Biometric Identification System (IDENT) with a SORN for EBR.[1]

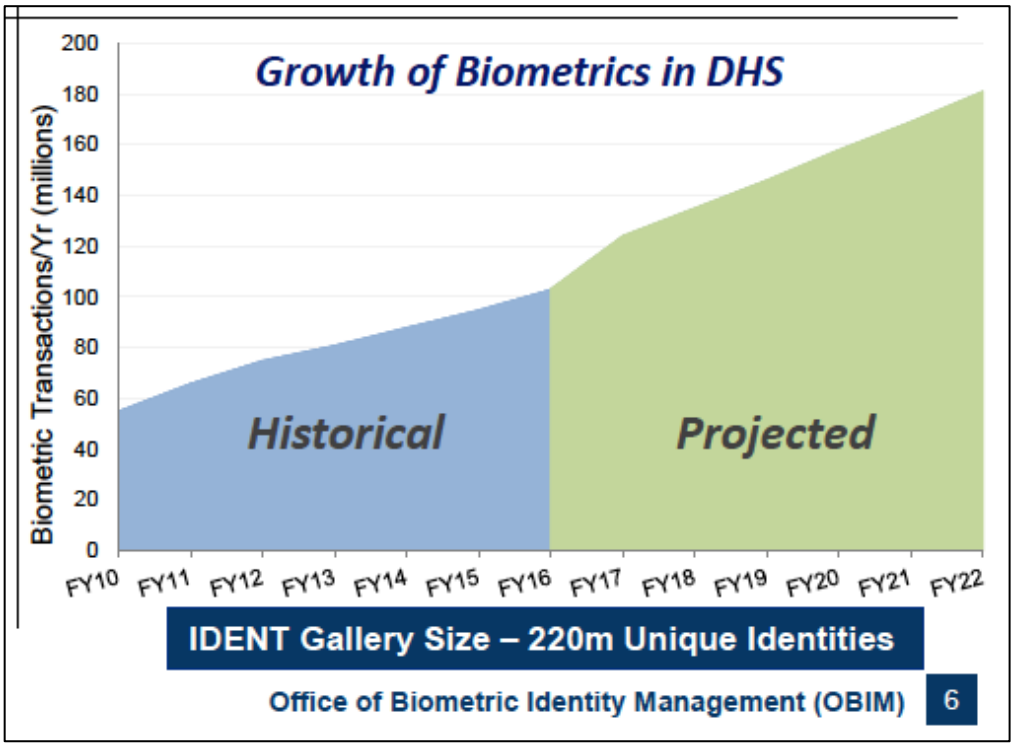
EFF is a member-supported, nonprofit, public interest organization dedicated to protecting privacy, civil liberties and innovation in the digital age. Founded in 1990, EFF represents the interests of tens of thousands of dues-paying members and the public in both court cases and broader policy debates surrounding the application of law in the digital age. EFF is particularly concerned with protecting privacy at a time when technological advances have resulted in increased surveillance by the government and actively encourages and challenges government and the courts to support privacy and safeguard individual autonomy as emerging technologies become prevalent in society.

INTRODUCTION

EFF files these comments to object to both the DHS's proposed Privacy Act exemptions and proposed System of Records Notice for the External Biometric Records (EBR) System of Records.

[1] *See* Department of Homeland Security, Notice of a new system of records, 83 Fed. Reg. 17829 (April 24, 2018) (hereinafter "Proposed DHS EBR SORN").

Growth of Biometrics at DHS[2]



Since the creation of DHS in 2002 and the publication of the SORN for DHS's legacy IDENT biometric database in 2007,[3] DHS has amassed a database of personal, biographic, and biometric data on millions of Americans and foreigners. According to DHS, IDENT is the largest biometric database in the United States. It contains more than 200 million unique biometric identities and processes more than 100 million biometric transactions every year. DHS also manages over 10 billion biographic records and adds 10-15 million more each week. DHS has created this massive database of personal data on millions of Americans and others with little congressional and public oversight. In fact, Congress expressed concern over the governance of DHS's Office of Biometric Identity Management (OBIM), withholding funds until its concerns could be addressed.[4]

---

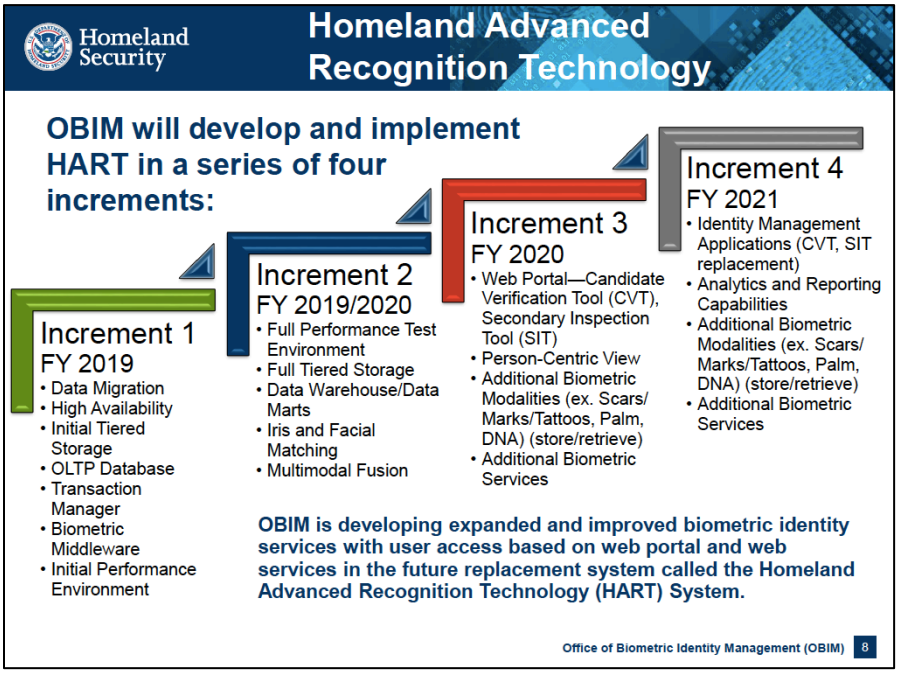
[2] Patrick Nemeth, *Identity Applications for Homeland Security*, DHS Office of Biometric Identity Management (Sept. 12, 2017) https://cloud.afcea.org/owncloud/s/ZcVv3ui0agn0HEn?path=%2FTrack%20A1%20and%20A2%20Identity%20Fundamentals#pdfviewer.

[3] *See* DHS/USVISIT-004 - DHS Automated Biometric Identification System (IDENT), 72 Fed. Reg. 31080 (June 5, 2007) https://www.gpo.gov/fdsys/pkg/FR-2007-06-05/html/07-2781.htm.

[4] CRS Report: DHS Appropriations FY2017: Protection, Preparedness, Response, and Recovery, 12 (Oct. 5, 2016 – Sept. 29, 2017) https://www.everycrsreport.com/files/20170929_R44660_dd11cfdbb3e035287198c5d660b5a133c4ae5a23.pdf.

Now DHS is building an even larger biometric database, called Homeland Advanced Recognition Technology (HART).[5]

Development Stages of DHS's HART Database [6]



The EBR SORN indicates HART will include not just DHS's own data, but also data from federal, state, and local agencies outside DHS as well as data from foreign governments. These data will be shared pursuant to "formal or informal" agreements that are opaque to the American public. DHS also plans to vastly expand the types of records it collects and stores to include at least seven different biometric identifiers, such as face and voice data, DNA, and a blanket category for "other modalities." Its system will also include "miscellaneous officer comment information" and "encounter data." And most importantly, DHS plans to collect and store data with broad First Amendment implications: "records related to the analysis of relationship patterns among individuals" including "non-obvious relationships."

DHS now asks the public to allow it to exempt this data from the important protections contained in the Privacy Act, essentially telling the public to trust it to ensure that the data is accurate. But the public has ample reason to question the accuracy of DHS's data and the data it obtains from non-DHS entities. To ensure that the risks to privacy and civil liberties presented by the vast trove of biometric data collected in the EBR system are minimized, DHS must produce a SORN that explains exactly what data is collected, how the data will be used, with whom it will be shared, and how it will be protected. Further, Americans must continue to have access to all their legal rights under the Privacy Act so that they may learn what data has been collected on them,

[5] *DHS reveals details of RFP for HART*, Planet Biometrics (Mar. 9, 2017), http://www.planetbiometrics.com/article-details/i/5614/desc/dhs-reveals-details-of-rfp-for-hart/.

[6] *See supra* n. 2.

determine that their own data is accurate, and ensure DHS is not collecting and using data in ways that violate the Act.

Because DHS's proposed SORN and Privacy Act exemptions fail to meet these requirements, we object to both.

I. DHS's External Biometric Records System

A. *Overview of the Proposed EBR System*

According to DHS, this proposed SORN covers records obtained from non-DHS entities, including Department of Justice, Department of Defense, State Department, and an unknown number of unlisted foreign and state and local entities with DHS relationships. The biometric records ingested into DHS's system will include faces, fingerprints (both deliberate and latent), iris scans, palm prints, voices, scars/tattoos, and DNA. The biometric data will be associated with biographic information, like name, date of birth, physical descriptors, country of origin, and government ID numbers. The system will also include "miscellaneous officer comment information" and "encounter data, including location and circumstance of each instance resulting in biometric collection." And the system will include data that tracks relationships among individuals.

The data in the system will not be limited to foreigners but will also include records on U.S. citizens and lawful permanent residents, two groups covered explicitly by the Privacy Act.

Given the sources of these data, including from the FBI's controversial Next Generation Identification database, they may be collected as part of a law enforcement or immigration investigation. However, the EBR system may also include data that is unrelated to these kinds of investigations. Instead it may have been collected and disclosed as part of a background check or licensing requirement for many types of jobs including, depending on the state, licensing to be a dentist, accountant, teacher, geologist, realtor, lawyer, or optometrist.[7] Since 1953, all jobs with

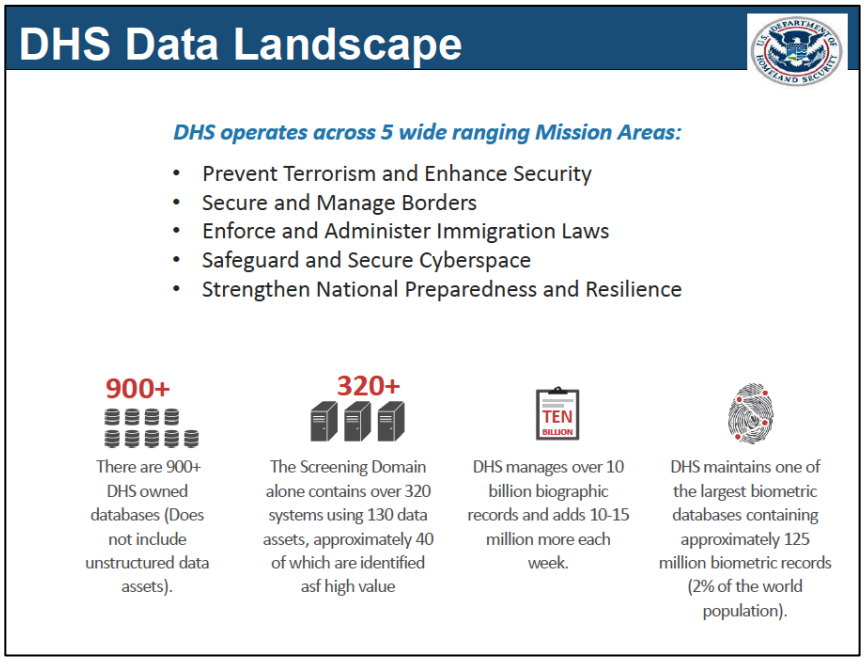
[7] *See, e.g.*, *Fingerprint Requirement for License Renewal*, Dental Bd. of Cal. (2016), http://www.dbc.ca.gov/licensees/fingerprint_faq.shtml#q1; *New Fingerprinting Process for CPA Exam Applicants*, Tex. St. Bd. of Publ. Acct. (Aug. 1, 2014), https://www.tsbpa.texas.gov/info/2014072801.html; *Completing the Fingerprint Requirement*, Wisc. Dept. of Pub. Instruction (Aug. 1, 2013), http://dpi.wi.gov/tepdl/licensing/fingerprint; *See Land Surveyors, and Geologists, Fingerprinting FAQ's*, Cal. Dept. of Consumer Aff. Bd. for Prof. Engineers (2012), http://www.bpelsg.ca.gov/applicants/fingerprinting_faqs.shtml; *Real Estate License Candidate Fingerprinting*, State of New Jersey Dept. of Banking & Insurance (Feb. 1, 2015), http://www.state.nj.us/dobi/division_rec/licensing/fingerprint.html; *Moral Character Determination Instructions*, The State Bar of Cal. (2016), https://www.calbarxap.com/applications/calbar/info/moral_character.html#fingerprints; *Fingerprint Requirement for License Renewal*, Cal. Dept. of Consumer Affairs Board of Optometry (June 21, 2010), http://www.optometry.ca.gov/faqs/fingerprint.shtml#q1.

the federal government have also required a fingerprint check, no matter the salary range or level of responsibility.[8]

B. *The Scope of the EBR System Is Far from Clear*

DHS notes that this SORN, along with a soon-to-be-published second SORN that covers only the technical aspects of the IDENT system, are intended to replace the 2007 SORN for the IDENT database. Since the 2007 IDENT SORN was published, DHS states it has moved to a federated approach to its data systems, producing separate SORNs to cover each of its components' data needs. However, this approach makes no sense when all components and non-DHS entities are submitting data to and reviewing data from a single biometric database such as HART. According to a recent DHS slide presentation, there are 900+ DHS-owned databases and over 320 systems. If DHS produces SORNs for each of these systems individually without a single unified SORN for the new HART system, it will make it exceedingly difficult for the American public to track and comment on the over-collection and overuse of biometric data by DHS.[9]

DHS Data Landscape[10]



[8] *See* Executive Order 10450: Security requirements for Government employment (Apr. 27, 1953), https://www.archives.gov/federal-register/codification/executive-order/10450.html.

[9] *Compare* FBI & DOJ, Notice of a Modified System of Records Notice, 81 Fed. Reg. 27284 (May 5, 2016) (hereinafter "FBI NGI SORN").

[10] DHS Immigration Data Integration Initiative Presentation (Sept. 14, 2017) https://cloud.afcea.org/owncloud/s/ZcVv3ui0agn0HEn?path=%2FTrack%20B%20-%20Special%20Sessions#pdfviewer.

This opportunity to comment on DHS's broader plans for biometric data is especially important, given recent indications that the agency believes it is legally authorized and is planning to collect and retain face data from millions of non-criminal U.S. citizens. According to the agency's own reports, DHS is partnering with private airlines to collect face recognition from all travellers leaving the country.[11] DHS has stated "the only way for an individual to ensure he or she is not subject to collection of biometric information when traveling internationally is to refrain from traveling."

However, many have questioned DHS's legal authority to collect and retain face recognition data from U.S. citizens and lawful permanent residents.[12] Senators Edward Markey and Mike Lee, in a recent letter addressed to the agency, stated, "[w]e are concerned that the use of the program on U.S. citizens remains facially unauthorized[.] . . . We request that DHS stop the expansion of this program and provide Congress with its explicit statutory authority to use and expand a biometric exit program on U.S. citizens."[13] As Georgetown's Center on Privacy and Technology notes, "while Congress has on nine separate occasions called on DHS to establish a 'biometric exit' program to verify the identities of foreign nationals as they leave the country, Congress has not authorized face scans of American citizens. DHS also has not established rules governing the program."[14] While DHS has recently proposed amending its regulations to provide that U.S. citizens may be required to provide photographs upon entering or departing the United States,[15]

---

[11] *Privacy Impact Assessment Update for the Traveler Verification Service (TVS): Partner Process*, DHS/CBP/PIA-030(c) (June 12, 2017).

https://assets.documentcloud.org/documents/3893766/TVS-PIA.pdf; *see also* Lee Fang & Ali Winston, "Private Companies Look to Cash in as Homeland Security Brings Facial Recognition to U.S. Borders," *The Intercept* (Nov. 29, 2017) https://theintercept.com/2017/11/29/facial-recognition-homeland-security-borders/.

[12] *See*, *e.g.*, Jay Stanley, "What's Wrong With Airport Face Recognition?," *ACLU* (Aug. 4, 2017) https://www.aclu.org/blog/privacy-technology/surveillance-technologies/whats-wrong-airport-face-recognition?redirect=blog/free-future/whats-wrong-airport-face-recognition; Jennifer Lynch, "TSA Plans to Use Face Recognition to Track Americans Through Airports" *EFF* (Nov. 9, 2017) https://www.eff.org/deeplinks/2017/11/tsa-plans-use-face-recognition-track-americans-through-airports.

[13] "Senators Markey and Lee Query Dept. of Homeland Security on Expansion of Facial Recognition Scanning Program at U.S. Airports" (Dec. 21, 2017) https://www.markey.senate.gov/news/press-releases/senators-markey-and-lee-query-dept-of-homeland-security-on-expansion-of-facial-recognition-scanning-program-at-us-airports.

[14] "Georgetown Privacy Center Issues New Report on Use of Facial Recognition Scans At Airports," (Dec. 21, 2017) http://www.georgetowntech.org/news-fullposts/2018/1/6/december-21-2017-georgetown-privacy-center-issues-new-report-on-use-of-facial-recognition-scans-at-airports.

[15] *See Proposed Rule: Collection of Biometric Data From U.S. Citizens Upon Entry To and Departure From the United States*, RIN: 1651-AB22 (Spring 2018) https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201804&RIN=1651-AB22.

this would do nothing to clarify the agency's legal (as opposed to regulatory) authority to collect this data.

Despite this, DHS appears ready to double-down on its data collection. CBP Commissioner Kevin McAleenan has stated CBP wants to be able to "confirm the identity of travelers at *any point in their travel*,"[16] not just at entry to or exit from the United States. Given CBP's recent partnerships with airlines, this could mean CBP plans to track travellers—possibly even U.S. citizens—from the moment they begin their internet travel research. The agency also wants to be able "to retrieve all associated traveler facial images from DHS holdings" and "fuse" this with biographic data into specific datasets.[17]

Given DHS's plans to collect and retain data from unspecified external partners, including information describing "relationship patterns," as well as its plans to track social media posts as part of its vetting program,[18] the scope of DHS's data collection appears unlimited. The SORN provides no data on what controls will be in place to ensure the data coming from other agencies are accurate, relevant, and not collected based on biased practices.

II. EBR Data is Inaccurate, Disproportionately Impacts People of Color, and Impinges on First Amendment Rights

A. *EBR Data Is Inaccurate and Has a Disproportionate Negative Impact on Communities of Color*

DHS has not taken necessary steps to determine whether the data collected from its external partners—states, other federal agencies, and foreign governments—are sufficiently accurate to prevent innocent people from being identified as criminal suspects, terrorists, or immigration law violators.

DHS has stated that it intends to rely on face recognition to identify data subjects across a variety of its mission areas,[19] and "face matching" is one of the first components of the HART database to be built out.[20] However, face recognition frequently is an inaccurate and unreliable biometric identifier. DHS's tests of its own systems found significantly high levels of inaccuracy.

---

[16] Testimony of Kevin K. McAleenan, Commissioner, C.B.P., "Border Security, Commerce and Travel: Commissioner McAleenan's Vision for CBP," 11 (April 25, 2018), https://docs.house.gov/meetings/HM/HM11/20180425/108207/HHRG-115-HM11-Wstate-McAleenanK-20180425.pdf.

[17] *Id*.

[18] Drew Harwell & Nick Miroff, "ICE just abandoned its dream of 'extreme vetting' software that could predict whether a foreign visitor would become a terrorist," *Wash. Post* (May 17, 2008), https://www.washingtonpost.com/news/the-switch/wp/2018/05/17/ice-just-abandoned-its-dream-of-extreme-vetting-software-that-could-predict-whether-a-foreign-visitor-would-become-a-terrorist/.

[19] *See*, *e.g.,* McAleenan Testimony "Border Security, Commerce and Travel: Commissioner McAleenan's Vision for CBP."

[20] *See supra* n. 6.

According to records released through FOIA, DHS's face recognition systems falsely reject as many as 1 in 25 travellers.[21] As a Georgetown report recently noted, "DHS' error-prone face scanning system could cause 1,632 passengers to be wrongfully delayed or denied boarding every day at New York's John F. Kennedy (JFK) International Airport alone."[22] Moreover, there is no indication that DHS has tested its system for false negatives, *i.e.*, whether people who are using fraudulent credentials are getting away with it. As a result, DHS has made no showing that its system is effective.

There is substantial evidence to suggest DHS's external partners are also employing face recognition systems with high rates of inaccuracy. For example, FBI has conducted only very limited testing to ensure the accuracy of NGI's face recognition capabilities,[23] and it admits in its PIA for the Interstate Photo System that IPS "may not be sufficiently reliable to accurately locate other photos of the same identity, resulting in an increased percentage of misidentifications."[24] In fact, FBI only ensures that "the candidate will be returned in the top 50 candidates" 85 percent of the time "when the true candidate exists in the gallery."[25] And a Government Accountability Office report on FBI's use of face recognition also notes that FBI's stated detection rate may not represent operational reality because FBI only conducted testing on a limited subset of images and failed to conduct additional testing as the size of its database increased. FBI also has never tested to determine detection rates where the size of the responsive candidate pool is reduced to a number below 50.[26]

FBI is not alone in employing an inaccurate face recognition system. Recently, advocacy organization Big Brother Watch discovered through Freedom of Information requests that several police departments in the United Kingdom were using face recognition systems with a false positive rate as high as a 98%—meaning that for every 100 people identified as suspects, 98 in fact were not suspects.[27] Using one of these systems, the Metropolitan Police misidentified

---

[21] "Senators Markey and Lee Query Dept. of Homeland Security on Expansion of Facial Recognition Scanning Program at U.S. Airports" (Dec. 21, 2017).

[22] Harrison Rudolph, et al, "Not Ready for Takeoff: Face Scans At Airport Departure Gates," Georgetown Center on Privacy & Technology (Dec. 21, 2017) https://www.airportfacescans.com/.

[23] *See* Government Accountability Office, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, 46, GAO-16-267 (May 2016) http://www.gao.gov/assets/680/677098.pdf (hereinafter "GAO Report"), at 26-27; Jennifer Lynch, *FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year*, and accompanying documents. https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year.

[24] *Privacy Impact Assessment for the Next Generation Identification (NGI) Interstate Photo System,* FBI, (Sept. 2015), https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/interstate-photo-system.

[25] *Id.*

[26] GAO Report, *supra* note 19, at 26.

[27] Big Brother Watch, *Face Off Campaign* (May 2018) https://bigbrotherwatch.org.uk/all-campaigns/face-off-campaign/.

95 people as criminals at a London street festival.[28] And a Welsh police department collected and stored photos of more than 2,400 innocent people incorrectly matched by face recognition for a year, without their knowledge. That agency plans to use this system again at a Rolling Stones concert next year. [29]

The number of false positives an identification system generates is especially important when those false positives represent real people who may become suspects in a law enforcement or immigration investigation.[30] False positives can alter the traditional presumption of innocence in these cases by placing more of a burden on suspects to show they are not who the system identifies them to be. This is true even if a face recognition system offers several results for a search instead of one; each of the people identified could be detained or brought in for questioning, even if there is nothing else linking them to a crime or violation. Former German Federal Data Protection Commissioner Peter Schaar has noted that false positives in face recognition systems pose a large problem for democratic societies: "[I]n the event of a genuine hunt, [they] render innocent people suspects for a time, create a need for justification on their part and make further checks by the authorities unavoidable."[31]

Technical issues endemic to all face recognition systems mean inaccurate results will continue to be a common problem for the foreseeable future. Face recognition technologies perform well when all the photographs are taken with similar lighting and shot from a frontal perspective (like a mug shot). However, when photographs that are compared to one another contain different lighting, shadows, backgrounds, poses, or expressions, the error rates can be significant.[32] Face recognition is also less accurate with large age discrepancies (for example, if a person is compared against a photo taken of himself when he was ten years younger). And it performs poorly with photographs taken at low resolutions and from a distance, so identifying an unknown face in a crowd from a large data set is particularly challenging.[33]

---

[28] *Id.*

[29] *Id*.

[30] Security researcher Bruce Schneier has noted that even a 90% accurate system "will sound a million false alarms for every real terrorist" and that it is "unlikely that terrorists will pose for crisp, clear photos." Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, 190 (2003).

[31] Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, 37, N.Y.U. (April 2009) http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf.

[32] *See, e.g.,* P. Jonathon Phillips, et al., "An Introduction to the Good, the Bad, & the Ugly Face Recognition: Challenge Problem," *National Institute of Standards & Testing* (Dec. 2011), *available at* www.nist.gov/itl/iad/ig/upload/05771424.pdf (noting only 15% accuracy for face image pairs that are "difficult to match").

[33] A 2009 New York University report concluded that, given these challenges, it is unlikely that face recognition systems with high accuracy rates under these conditions will become an "operational reality for the foreseeable future." Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, p. 3, N.Y.U. (April

Most importantly, face recognition has an unfair disproportionate impact against African Americans and other people of color. Research—including research jointly conducted by one of the FBI's senior photographic technologists—has shown that face recognition misidentified African Americans and ethnic minorities, young people, and women at higher rates than whites, older people, and men, respectively.[34] Recent research from MIT found significant error rates across face recognition systems for darker-skinned African Americans and especially for African American women.[35] Moreover, due to years of well-documented racially-biased police and immigration practices, all criminal databases—including mugshot databases—unjustifiably include a disproportionate number of African Americans, Latinos, and immigrants.[36] Also, in many communities, police have deployed surveillance cameras more heavily in minority neighborhoods than in white neighborhoods—meaning minority residents will more often be subjected to face recognition. These facts mean people of color will shoulder exponentially more of the burden of face recognition inaccuracies than whites.

EBR's disparate impact is not limited to face recognition inaccuracy, because law enforcement records as a whole, which the EBR system will include, are also notoriously unreliable. For example, at least 50% of FBI's arrest records fail to include information on the final disposition of the case—whether a person was convicted, acquitted, or if charges against them were dropped.[37] Because at least one-third of people arrested for a felony are never charged with or

---

2009) http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf. Recently, Russian developers announced that their system, called FindFace, could identify a person on the street with about 70% accuracy if that person had a social media profile. However, it is unclear at what resolution and distance the probe photos were taken and how many images of each person were available to compare the probe photos against (more photographs taken from different angles and under different lighting conditions could increase the probability of a match). *See, e.g.*, Ben Guarino, *Russia's new FindFace app identifies strangers in a crowd with 70 percent accuracy*, Wash. Post (May 18, 2016) https://www.washingtonpost.com/news/morning- mix/wp/2016/05/18/russias-new-findface-app-identifies-strangers-in-a-crowd-with-70- percent-accuracy/.

[34] *See* R. W. Vorder Bruegge, et al., *Face Recognition Performance: Role of Demographic Information*, 7 IEEE Transactions on Info. Forensics and Sec. 6, 1789-1801(Dec. 2012), http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6327355&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Ficp.jsp%3Farnumber%3D6327355.

[35] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research* (2018) http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. This problem is due in part to the fact that people of color and women are underrepresented in training data.

[36] *See Criminal Justice Fact Sheet*, NAACP (2009), http://www.naacp.org/criminal-justice-fact-sheet.

[37] *See* Madeline Neighly & Maurice Emsellem, *WANTED: Accurate FBI Background Checks for Employment*, National Employment Law Project (July 2013) *available at* http://www.nelp.org/content/uploads/2015/03/Report-Wanted-Accurate-FBI- Background-Checks-Employment.pdf. *See also* Ellen Nakashima, "FBI Wants to Exempt Its Huge Fingerprint and Photo Database from Privacy Protections," *Washington Post* (June 30, 2016) https://www.washingtonpost.com/world/national-security/fbi-wants-to- exempt-its-huge-

convicted of any crime,[38] this means a high percentage law enforcement records incorrectly indicate a link to crime.

Likewise, DHS's own immigration data has also been shown to be unacceptably inaccurate. A 2005 Migration Policy Institute study analyzing records obtained through FOIA found "42% of NCIC immigration hits in response to police queries were 'false positives' where DHS was unable to confirm that the individual was an actual immigration violator."[39] A 2011 study of DHS's Secure Communities program found approximately 3,600 United States citizens were improperly caught up in the program due to incorrect immigration records.[40]

B. *The EBR System Will Burden First Amendment Rights*

The collection, retention, and sharing of EBR will intrude on First Amendment-protected activities and will chill speech. It could also violate a key provision of the Privacy Act designed to prevent data collection on First Amendment protected activities.[41] The vast array of data sources for EBR would mean that anyone could end up in the database without their knowledge—even if they're not suspected of a crime or legal violation—by just happening to be in the wrong place at the wrong time or by fitting a stereotype that some in society have decided is a threat.

Biometrics programs that collect, store, share, and combine sensitive and unique data pose critical threats to privacy and civil liberties. Our biometrics are unique to each of us, can't be changed, and often are easily accessible. Face recognition, though, takes the risks inherent in other biometrics to a new level because it is much more difficult to prevent the collection of an image of one's face. Most of us expose our faces to public view every time we go outside, and many of us share images of our faces online with almost no restrictions on who may access our images. Face recognition therefore allows for covert, remote, and mass capture and identification

---

fingerprint-and-photo-database-from-privacy- protections/2016/05/31/6c1cda04-244b-11e6-8690-f14ca9de2972_story.html (noting that, according to FBI, "43 percent of all federal arrests and 52 percent of all state arrests — or 51 percent of all arrests in NGI — lack final dispositions").

[38] Amy L. Solomon, *In Search of a Job: Criminal Records as Barriers to Employment*, NIJ Journal No. 270 (June 2012) https://www.nij.gov/journals/270/pages/criminal-records.aspx.

[39] National Immigration Law Center, *Untangling the Immigration Enforcement Web*, 7-8 (Sept. 2017) https://www.nilc.org/wp-content/uploads/2017/09/Untangling-Immigration-Enforcement-Web-2017-09.pdf.

[40] Aarti Kohli, et al., *Secure Communities by the Numbers: An Analysis of Demographics and Due Process*, at p.4, Chief Justice Earl Warren Institute on Law and Social Policy, UC Berkeley School of Law (Oct. 2011), available at www.law.berkeley.edu/files/Secure_Communities_by_the_Numbers.pdf.

[41] *See* 5 U.S.C. 552a(e)(7) (forbidding agencies from maintaining "records 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").

of images[42]—and the photos that may end up in a database could include not just a person's face but also how she is dressed and possibly whom she is with.

Face recognition and the accumulation of easily identifiable photographs implicate free speech and freedom of association rights under the First Amendment, especially because face-identifying photographs of crowds or political protests can be captured in public, online, and through public and semi-public social media sites without individuals' knowledge.

Law enforcement has already used face recognition technology at political protests. Marketing materials from the social media monitoring company Geofeedia bragged that, during the protests surrounding the death of Freddie Gray while in police custody, the Baltimore Police Department ran social media photos against a face recognition database to identify protesters and arrest them.[43]

DHS compounds the threats to free speech posed by the collection of face data in several ways. First, DHS defines EBRs to include "records related to the analysis of relationship patterns among individuals" including "non-obvious relationships." Second, these records include "encounter data," which frequently means information collected by police during interactions with civilians when there is no individualized suspicion of crime. Worse, this data is often collected under extremely questionable legal circumstances. For example, ICE officers use mobile devices to collect biometric and biographic data from people they "encounter" in the field, including via unauthorized entry into people's homes and bible study groups, and in public places where people congregate with other members of their community, such as on soccer fields, in community centers, and on buses.[44] Finally, DHS uses gang databases (its own and those from states), which often contain unsubstantiated data concerning people's status and associations and are notoriously inaccurate.[45]

Finally, studies show that surveillance systems and the overcollection of data by the government chill expressive and religious activity. For example, in 2013, a study involving Muslims in New York and New Jersey found excessive police surveillance in Muslim communities had a significant chilling effect on First Amendment-protected activities.[46] Specifically, people were less inclined to attend mosques they thought were under government surveillance or to engage in

---

[42] *See* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 Minn. L. Rev. 407, 415 (Dec. 2012).

[43] *Baltimore County Police Department and Geofeedia Partner to Protect the Public During Freddie Gray Riots*, Geofeedia, https://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf.

[44] National Immigration Law Center, *Untangling the Immigration Enforcement Web*, 13-14 (Sept. 2017).

[45] *Id.* at 11-12. (noting the CalGangs database included listings for 42 infants less than a year old, 28 of whom "admitted" to being gang members).

[46] Diala Shamas & Nermeen Arastu, *Mapping Muslims: NYPD Spying and its Impact on American Muslims* (Mar. 2013), http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

religious practices in public, or even to dress or grow their hair in ways that might subject them to surveillance based on their religion. People were also less likely to engage with others in their community who they didn't know for fear any such person could either be a government informant or a radical. Parents discouraged their children from participating in Muslim social, religious, or political movements. Business owners took conscious steps to mute political discussion by turning off Al-Jazeera in their stores, and activists self-censored their comments on Facebook.[47]

III. The EBR System Should Not be Exempted from the Privacy Act

EFF objects to both the proposed SORN and the proposed Privacy Act Exemptions. As discussed above, the extremely sensitive and private nature of this data requires DHS to issue a SORN that explains clearly what data is collected on individuals, under what circumstances, how that data is used, and with whom it is and will be shared. The proposed SORN is overly vague and fails to meet these base-level requirements.

Further, DHS should not exempt EBR data from key provisions of the Privacy Act. The nature and vast quantity of the data collected, combined with DHS's demonstrated failure to maintain accurate and up-to-date records, show why Americans must continue to have access to the full protections of the Privacy Act.

DHS proposes to exempt much of the EBR database from three key provisions of the Privacy Act: (1) the right to access records maintained on oneself; (2) the right to ensure that those records are maintained accurately and to be able to correct inaccuracies; and (3) the right to know with whom one's data is being shared.

The Privacy Act requires DHS to not only maintain accurate records but also to ensure that the information it collects from and disseminates to other federal and non-federal agencies is "accurate, complete, timely and relevant." DHS's Office of Biometric Identity Management (OBIM), the agency component responsible for managing DHS's biometric systems, recognizes privacy is "essential to the program mission."[48] OBIM states it "takes privacy into account from conception through planning and development, and during the execution of every aspect of the OBIM program."[49] Nevertheless, as discussed above, DHS's records have, in the past, contained significant inaccuracies that impact Americans' lives, and its proposed inclusion of large numbers of EBRs will only contribute to this problem.

DHS's proposed exemptions seek to prevent Americans from ever knowing exactly what data the Department maintains on them and shares with other agencies. And, by seeking to remove any judicial remedy, the exemptions attempt to prevent Americans from ensuring that the data the Department maintains is "accurate, complete, timely and relevant."

---

[47] *Id*.

[48] DHS, Office of Biometric Identity Management: Privacy Information, https://www.dhs.gov/obim-privacy-information.

[49] *Id.*

This has real-world consequences. For example, as discussed above, due to notoriously inaccurate and out-of-date immigration and arrest records,[50] several thousand U.S. citizens were caught up in the "Secure Communities" program—a program that resulted in detention and deportation for hundreds of thousands of people.[51] DHS's proposed exemptions would take away the ability for citizens in cases such as these to learn whether the inaccurate records leading to their detention came from the agency. They would also remove those citizens' rights to compel DHS to correct and update its records.

Given the vast scope of data included in EBR, the impact that inaccuracies in that data would have on Americans' lives, and the possibility DHS and other agencies may use this data—in violation of the Privacy Act—to monitor First Amendment protected activities, DHS should not be allowed to exempt EBR from the Privacy Act.

IV. The SORN is Overly Vague and Fails to Specify Exactly Which Records Are Maintained in the System

The Privacy Act requires federal agencies that maintain records on individuals to publish a SORN that describes whose records are included in the system, what types of records are included, who has access to those records and for what purpose, and the "policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records."[52] DHS's proposed SORN for the EBR System is impermissibly vague and fails to meet these basic requirements.

Specifically, the following sections fail to meet the requirements of the Privacy Act.

1. *Purposes*

This section states that some of the purposes for maintaining data in EBR are "national security," "intelligence," and "national defense." The section also refers to unspecified "foreign and domestic" "non-DHS entities" as well as an undefined "agreement or arrangement." These terms are unclear and not properly limited in scope.

---

[50] S*ee generally* Joan Friedland, National Immigration Law Center, *INS Data: The Track Record*, *available at* www.nilc.org/document.html?id=233 (citing multiple Government Accountability Office and Inspector General reports on inaccuracies in immigration records). These problems persist. *See generally, e.g,* U.S. Government Accountability Office (GAO), *Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain*, GAO-11-146 (Jan. 18, 2011), *available at* http://www.gao.gov/products/GAO-11-146 (noting errors in USCIS's e-Verify system and difficulties in correcting those errors).

[51] *See, e.g.,* Aarti Kohli, et al. *Secure Communities by the Numbers: An Analysis of Demographics and Due Process*, *supra* n. 40.

[52] 5 U.S.C. 552a(e)(4).

2. *Categories of Individuals Covered by the System:*

This section states that the EBR system includes individuals whose biometric and biographic information was collected by non-DHS agencies for purposes including "national security," "law enforcement operations," "intelligence," and "national defense." This definition is circular, vague, and impermissibly broad because it defines individuals covered by the system as individuals whose data is included in the system. It thus fails to place any meaningful limits on the types of data that may be included in the EBR system or the people who may be swept up into the system. It also fails to explain to individuals the reason(s) for their biometric and biographic data ending up in the system.

Furthermore, the system could include data gathered on people lawfully engaged in First Amendment protected speech. State and federal law enforcement agencies regularly investigate political protests in the physical world and conduct investigations in virtual "locations" online. The collection and retention of this data implicates First Amendment protected activity and freedom of association. However, it appears this section would allow DHS to maintain these sensitive records in the EBR system merely by stating they are associated with "law enforcement operations." The SORN needs to assure Americans that data collected from other agencies based on First Amendment-protected activities will not end up in the EBR system absent a documented probable cause warrant and judicial authorization.

3. *Record Source Categories*

The SORN states that DHS includes data in EBR that it receives from "foreign partners consistent with various international information sharing and access agreements or arrangements on file with DHS Office of Policy, International Affairs." Similarly, it states data comes from "State and local partners consistent with various law enforcement information sharing and access agreements or arrangements." These sections are vague and impermissibly broad, fail to delineate what kinds of agreements control when data is entered into EBR, and fail to state clearly how these arrangements can be examined.

4. *Routine Uses*

This section includes many terms that are all vague and fail to properly explain which records are shared, under what circumstances they may be shared, and with whom. For ease of discussion, all overly vague terms are highlighted below in italics:

> H. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, *when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law*, which includes criminal, civil, or regulatory violations and such disclosure is proper and *consistent with the official duties* of the person making the disclosure.
>
> J. To a Federal, State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order

> to *provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities* authorized by U.S. law, Executive Order (E.O.), or other applicable national security directive.
>
> N. 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 a clearly unwarranted invasion of personal privacy.

5. *Policies and Practices for Storage of Records; Administrative, Technical, and Physical Safeguards:*

The Storage Procedures and Safeguards sections state the following:

> DHS stores records in this system electronically in secure facilities protected through multi-layer security mechanisms and strategies that are physical, technical, administrative, and environmental in nature. The records may be stored on magnetic disc, tape, and digital media.
>
> DHS safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

This section fails to specify exactly how the sensitive, private information contained in the EBR system will be protected. The many recent security breaches and reports of falsified data—including biometric data—show that the government must have extremely rigorous security measures and audit systems in place to protect against data loss. For example, in 2017, hackers took over 123 of Washington D.C.'s surveillance cameras just before the presidential inauguration, leaving them unable to record for several days.[53] During the 2016 election year, news media were consumed with stories of hacks into email and government systems, including into United States political organizations and online voter registration databases in Illinois and

[53] Rachel Weiner, *Romanian hackers took over D.C. surveillance cameras just before presidential inauguration, federal prosecutors say*, Wash. Post (Dec. 28, 2017), https://www.washingtonpost.com/local/public-safety/romanian-hackers-took-over-dc-surveillance-cameras-just-before-presidential-inauguration-federal-prosecutors-say/2017/12/28/7a15f894-e749-11e7-833f-155031558ff4_story.html.

Arizona.[54] And in 2015, sensitive data stored in Office of Personnel Management (OPM) databases on more than 25 million people was stolen,[55] including biometric information and addresses, health and financial history, travel data, and data on people's friends and neighbors.[56] More than anything, these breaches have exposed the vulnerabilities in government systems to the public—vulnerabilities that the United States government appears to have known for almost two decades might exist.[57]

It is unclear whether federal agencies have done much to improve the security of their systems since these breaches. Given the government's poor track record on securing data and the fact that DHS intends to retain personal data in EBR for up to seventy-five years,[58] DHS must do more than publish two short paragraphs to explain how it will safeguard the sensitive biometric and biographic data contained in EBR.

CONCLUSION

EBR appears to represent a fundamental change in the type and quality of data the federal government is collecting and retaining on individuals as well as a sharp increase in data collection and retention overall. Consequently, the public must know how that data is collected, used, and shared and be able to ensure that DHS is complying with its legal responsibilities under the Privacy Act. DHS's proposals to exempt the EBR system from key sections of the Privacy Act would prevent that from happening. For these reasons, EFF objects to both the DHS's proposed Privacy Act Exemptions and proposed System of Records Notice for the EBR System of Records.

Contact: *Jennifer Lynch, Senior Staff Attorney, Electronic Frontier Foundation*

---

[54] *See, e.g.,* Tracy Connor, et al., *U.S. Publicly Blames Russian Government for Hacking*, NBC News (Oct. 7, 2016), http://www.nbcnews.com/news/us-news/u-s-publicly-blames-russian-government-hacking-n662066.

[55] Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. Times (July 9, 2015), http://www.nytimes.com/2015/07/10/ us/office-of-personnel-management-hackers-got-data-of-millions.html; *See also, e.g.,* David Stout and Tom Zeller Jr., *Vast Data Cache About Veterans Is Stolen*, N.Y. Times (May 23, 2006), https://www.nytimes.com/2006/05/23/washington/23identity.html; *See also MEPs question Commission over problems with biometric passports*, European Parliament News (Apr. 19, 2012), http://www.europarl.europa.eu/news/en/headlines/content/20120413STO42897/html/MEPs-question-Commission-over-problems-with-biometric-passports (noting that, at the time, "In France 500,000 to 1 million of the 6.5 million biometric passports in circulation are estimated to be false, having been obtained on the basis of fraudulent documents").

[56] *Id.*

[57] *Id*.

[58] *See* Proposed DHS EBR SORN, "Policies and Practices for Retention and Disposal of Records."