WORLD **PRIVACY** FORUM

The Honorable Kirstjen M. Nielsen
Secretary of Homeland Security
Washington, D.C. 20528

Sam Kaplan
Chief Privacy Officer
US Department of Homeland Security

September 18, 2018

RE: Regulatory, Legal and Policy Concerns with Biometric Entry and Exit Program

Dear Secretary Nielsen and Mr. Kaplan:

This letter outlines our substantive concerns regarding the US Department of Homeland Security (DHS) Customs and Border Protection (CBP) and Transportation Security Administration (TSA) biometric[1] entry and exit program. The World Privacy Forum[2] calls on the Secretary to provide formal notice and solicit public comments pursuant to the Administrative Procedure Act, and to address and resolve the additional regulatory, legal and policy issues we discuss in this letter.

Although DHS issued three Privacy Impact Assessments regarding this program, DHS failed to provide formal notice and solicit public comments pursuant to requirements of the Administrative Procedure Act (APA) for its Phase I and Phase II pilot tests of the biometric entry and exit system. DHS failed to do so despite an extensive implementation of the stage II pilot of biometric technology at many airports with international flights, affecting millions of travelers annually.

This letter focuses on the specific problems of legal liabilities of the biometric entry and exit program, the lack of availability of redress under APA before programs are

[1] In this letter, *biometric* refers to automated recognition of individuals based on their biological and/or behavioral characteristics. There are many types of biometrics. For example facial recognition systems are a type of biometric, as are systems that include fingerprint analysis, iris recognition, and gait analysis. In this letter, we primarily discuss facial recognition biometric systems. See: International Organization for Standardization: Information technology, Vocabulary, Part 37: Biometrics. ISO/IEC 2382-37:2017, JTC 1/SC 37, Geneva, Switzerland, 2017. Available at: https://www.iso.org/standard/66693.html.

[2] The World Privacy Forum is a non-profit public interest research and consumer education group focusing on issues related to consumer privacy and data protection. Our work includes substantive, original, peer-reviewed research in the field of biometrics as it relates to privacy. Our work may be found at www.worldprivacyforum.org.

implemented, and the applicability of the Violence Against Women Act (VAWA) to these programs. This letter also identifies further implementation concerns regarding ownership of airport cameras, complex and unmapped data flows, and the role of biometric data sharing with commercial entities without adequate contractual or privacy controls.

The Chief Privacy Officer (CPO) of DHS has full authority to identify problems in systems and to make sure that DHS components address them. The CPO has primary responsibility under Section 222 of the Homeland Security Act of 2002, as amended, for privacy policy at DHS. This responsibility includes assuring that the use of technologies sustains and does not erode privacy protections relating to the use, collection, or disclosure of personal information. The CPO has the authority to require DHS employees to comply with policies to ensure that all individuals have suitable privacy protections, regardless of citizenship and immigration status, in compliance with E.O. 13,768, for personally identifiable information (PII) collected, used, retained, or disseminated by DHS. Pursuant to this responsibility, the law requires that the Fair Information Practices[3] serve as the framework for privacy policy and implementation at DHS.[4]

We request that you conduct a rigorous assessment of the CBP biometric entry and exit systems regarding the problems we discuss in this letter.

I. Failure of the biometric entry and exit Phase I and Phase II expanded implementations to comply with public notice and comment requirements of the Administrative Procedures Act

DHS has not yet provided for public notice and comment pursuant to the requirements of the Administrative Procedures Act (APA) for the biometric entry and exit program. Sections 553(b) and (c) of the APA require an agency to publish notice of a proposed rule in the Federal Register and to solicit and consider public comments upon its proposal. The narrow exceptions to this rule, codified in § 553(b)(3)(A), do not apply "to interpretative rules, general statements of policy, or rules of agency organization, procedure, or practice." The CBP decision to use biometric screenings does not fit these exclusions because it requires a substantive change in procedures at checkpoints and at the point of boarding international flights.

The biometric entry and exit program requires *new* information collections and uses from CBP, TSA, and additional non-governmental information collection by the airlines. Moreover, the consequences for all the individuals affected by this new procedure are profound and not limited solely to use by CBP itself. First, other government agencies will also use the biometric data. Second, biometric information collected by the airlines

[3] Gellman, Robert, Fair Information Practices: A Basic History (April 10, 2017). Available at SSRN: https://ssrn.com/abstract=2415020 or http://dx.doi.org/10.2139/ssrn.2415020.
[4] Jonathan Cantor, Acting Chief Privacy Officer, Privacy Policy Guidance Memorandum, Memorandum Number: 2017-01. Department of Homeland Security, April 27, 2017. Available at: https://www.dhs.gov/sites/default/files/publications/Privacy%20Policy%20Guidance%20Memo%202017-01%20-%20FINAL.pdf.

and held in their possession does not fall under the protections of the Privacy Act of 1974. The airlines, even though they are presumably collecting biometric information for use by CBP, can subsequently use the information for secondary purposes unrelated to the CBP.

All of these matters create new, significant intrusions on privacy and create meaningful changes that impose upon millions of members of the public to a degree that requires notice-and-comment rulemaking.

The entry and exit program is now in "Phase II expanded pilot," which is a euphemism for an actual implementation, nearly nationally now, and soon to be in all airports with international flights by the end of 2018.[5] Directly relevant legal precedent requires that DHS immediately cease further implementation and provide public notice and comment *now*. Although DHS issued a Paperwork Reduction Act (PRA) notice and comment,[6] this type of notice and comment is not equivalent to compliance with the APA. A comment period under the PRA does not absolve DHS from undertaking a full notice and comment period under the APA.

The examination of directly relevant legal precedent makes clear that the federal courts apply APA procedure to such a substantive new collection and dissemination of PII of the traveling public. In *EPIC vs. DHS*,[7] the D.C. Circuit court found that the TSA could not justify its failure to provide notice and comment for the TSA's body scanner system. In the suit, EPIC argued that the Transportation Security Administration proposal to implement a body scanner program for security screening of travelers in US airports should have been the subject of a formal notice-and-comment rulemaking ***prior*** to implementation of scanners in airports. The government, for its part, argued that it did not need to undertake formal notice and comment prior to installing body scanners for passenger screening at airports.

The government made three procedural arguments as to why the department was not required to undergo a comment period. The majority decision expressly dealt with all three procedural arguments raised in defense of TSA's program and explicitly found them insufficient. The Court required TSA to follow the APA's notice-and-comment process.[8]

---

[5] Ron Nixon, *Facial Scans at U.S. Airports Violate Americans' Privacy, Report Says.* New York Times, Dec. 21, 2017. "...homeland security officials begin to roll out a biometric exit system that uses facial recognition scanning in 2018 at all American airports with international flights." https://www.nytimes.com/2017/12/21/us/politics/facial-scans-airports-security-privacy.html.

[6] 83 FR 24326 https://www.federalregister.gov/documents/2018/05/25/2018-11287/agency-information-collection-activities-biometric-identity.

[7] *Electronic Privacy Information Center v. US Department of Homeland Security* (D.C. Cir. 2011), https://epic.org/privacy/body_scanners/EPIC_v_DHS_Decision_07_15_11.pdf.

[8] *Electronic Privacy Information Center v. US Department of Homeland Security* (D.C. Cir. 2011), https://epic.org/privacy/body_scanners/EPIC_v_DHS_Decision_07_15_11.pdf. "To sum up, first, we grant the petition for review insofar as it claims the TSA has not justified its failure to initiate notice-and-comment rulemaking before announcing it would use AIT scanners for primary screening. None of the exceptions urged by the TSA justifies its failure to give notice of and receive comment upon such a rule, which is legislative and not merely interpretive, procedural, or a general statement of policy. Second, we

The *EPIC vs. DHS* decision lays unambiguous groundwork for legal action against DHS should DHS not immediately satisfy the legal requirements for notice and comment on the Customs and Border Protection system as well as the TSA biometric entry and exit system, Pilot Phase I and now the expanded Phase II pilot. The impact on air travelers is substantial, and what is being called an expanded Phase II Pilot is, as we argue later, in fact the equivalent of actual implementation. The reality of the program, rather than its label, is the determining factor for the timing of the notice and comment requirement.

The time for notice and comment under the APA is right now, not later. It is already late, and an expanded Phase II pilot should not proceed further without a public notice and comment period.

II. The biometric entry and exit program constitutes a meaningful, nation-wide implementation, and no longer qualifies as a "pilot" or technical demonstration

The biometric entry and exit program, which CBP describes as a "technical demonstration" in its PIAs, is currently in 16 total US airports, and air entry (preclearance) is available in 4 overseas airports.[9] In 2018, the program is set to roll out to *all US airports with international flights*.[10] Yet despite the projected full rollout of the program, CBP has thus far ignored its obligation under the APA and the clear legal holding articulated in *EPIC v. DHS*.

(See Appendix B for a chart of all airports listed as of September 18, 2018 as participating in biometric air exit and entry.)

Additionally, on its website, CBP states that it has begun actual *implementation* of the program:

> CBP has begun implementation of Biometric Air Exit. Either CBP or airline

---

deny the petition with respect to the petitioners' statutory arguments and their claim under the Fourth Amendment, except their claim under the RFRA, which we dismiss for lack of standing. Finally, due to the obvious need for the TSA to continue its airport security operations without interruption, we remand the rule to the TSA but do not vacate it, and instruct the agency promptly to proceed in a manner consistent with this opinion."

[9] According to the CBP website, biometric air exit is available at 14 airports, biometric air exit is available at 12 airports, and biometric entry is available at 8 US airports and 4 overseas participants in preclearance. See: CBP, https://www.cbp.gov/travel/biometrics. *See also*: Aaron Boyd, Using Homeland Security's biometric program, one airport is increasing security while shortening lines. NextGov, June 25, 2018. Available at: https://www.nextgov.com/emerging-tech/2018/06/us-customs-expects-face-scanning-speed-security-florida-airport/149256/. *See also*: Hillary Grigonis, US Customs says biometric entry and exit is coming first to this airport. Digital Trends, June 22, 2018. Available at: https://www.digitaltrends.com/cool-tech/biometric-entry-and-exit-at-orlando/.

[10] Ron Nixon, *Facial Scans at U.S. Airports Violate Americans' Privacy, Report Says.* New York Times, Dec. 21, 2017. "...homeland security officials begin to roll out a biometric exit system that uses facial recognition scanning in 2018 at all American airports with international flights." https://www.nytimes.com/2017/12/21/us/politics/facial-scans-airports-security-privacy.html.

.

> partners will take photographs of passengers while boarding international departing aircraft from the U.S. The purpose is to confirm that each passenger is the true bearer of the travel document required for travel. In addition, for non-U.S. citizens, the photograph will be used as biometric confirmation of departure from the United States, as required by law (8 U.S. Code § 1365b).[11]

The CBP entry and exit program can no longer reasonably be described as merely a pilot or demonstration project. Flights from a few airports for a period of one year or less could reasonably constitute pilot testing. DHS has deployed the technology now for several years, and plans to deploy it in 2018 in *every airport in the US with international flights*. This is not what a pilot test looks like. The technology is materially affecting passengers, as detailed in CBP's own documentation of the program, in which it states that not all privacy risks have been mitigated.[12] Given this admission by DHS, it is impermissible for CBP to not have already given the public a full notice and comment period. The changes to passenger screening brought about by the widespread -- and soon to be universal implementation of this program -- substantively affect the public to a degree sufficient as to require notice-and-comment rulemaking.

The DHS failure to seek public comment before further significant installment of the technology is particularly important because both of the Privacy Impact Assessments from Phase I and Phase II identified clear privacy risks to passengers from the program.[13] Moreover, we identify here additional risks for victims of crime and domestic violence, risks that CBP did not raise or address in its PIAs related to the biometric entry and exit program.

This program cannot plausibly be deemed a pilot because CBP has stated that it has begun implementation of biometric exit.[14] CBP has also described the program as

---

[11] See US Customs and Border Protection, Biometric Air Exit Page. Last accessed September 18, 2018. Available at: https://www.cbp.gov/travel/biometrics/air-exit.

[12] See US Department of Homeland Security, Privacy Impact Assessment, Privacy Impact Assessment Update for the Traveler Verification Service (TVS): CBP-TSA Technical Demonstration Phase II DHS/CBP/PIA-030(e) (August 14, 2018), available at: https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030e-tvs-august2018_0.pdf. *See also:* US Department of Homeland Security, Privacy Impact Assessment, Traveler Verification Service (TVS): Partner Process DHS/CBP/PIA-030(c) June 12, 2017. Available at: https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-june2017.pdf. *See also*: US Department of Homeland Security, Privacy Impact Assessment Update for the Traveler Verification Service (TVS):CBP TSA Technical Demonstration DHS/CBP/PIA-030(d)September 25, 2017. Available at: https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-september2017.pdf.

[13] US Department of Homeland Security, Privacy Impact Assessment, Traveler Verification Service (TVS): Partner Process, DHS/CBP/PIA-030(c) June 12, 2017. Available at: https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-june2017.pdf. For Phase II, see, US Department of Homeland Security, Privacy Impact Assessment, Privacy Impact Assessment Update for the Traveler Verification Service (TVS): CBP-TSA Technical Demonstration Phase II DHS/CBP/PIA-030(e) (August 14, 2018), available at: https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030e-tvs-august2018_0.pdf.

[14] *Supra* note 11.

mandatory to some travelers.[15] In a 2016 press release about the commencement of the biometric exit program at the Hartsfield-Jackson Atlanta airport, CBP stated:

> As part of the testing, travelers will present their boarding pass while their digital photo is taken. The process will take less than three seconds before travelers proceed to the passenger loading bridge to board their flight. **Travelers over the age of 14 and under 79 will be required to participate in the test.** The test will evaluate CBP's ability to successfully compare the image of a traveler taken during departure against an image the traveler previously provided, in an automated fashion and without impacting airport operations. [Emphasis ours.][16]

This action alone is sufficient to trigger DHS' public notice-and-comment obligations. In 2017, CBP backtracked from this position slightly, using its issuance of a Privacy Impact Assessment (PIA) and the *de minimis* addition of airport signage as a fig leaf for its prior lack of notice. We do not believe that the airport signage in use allows DHS to argue with a straight face that the program is somehow voluntary. The signage we have seen (See Appendix A for a screenshot of sample signage) does not clearly indicate voluntariness, and is not thorough in its notice. After previously describing participation as mandatory for the traveling public, simply rebranding the program does not vitiate the requirements that a full notice and comment period is required prior to implementation pursuant to the plain language of the APA.

III. Policy before Technology; APA notice and comment before implementation of biometric programs is a necessity

The availability of redress under the APA ***before*** program implemention is critical. Meaningful privacy risks for passengers arise from this program, as well as additional risks -- including technical security risks related to biometrics -- that CBP has not included in its risk analysis in its published PIAs. CBP and its proposed biometric entry and exit program would, along with the public, be a clear beneficiary of public comments. Feedback from biometric experts will make the program better. Feedback from at-risk stakeholders such as victims of crime and domestic violence will make the program safer for survivors and those using airports to get to safety. Feedback from privacy experts will provide a much more thorough assessment of risks, including data

---

[15] The program has been mandatory for a selection of passengers since at least 2016. For all intents and purposes it remains so now, with notice to passengers that is generally not prominent. Additionally, from 2016 to part of 2017, passengers did not receive notice at all, but they were still required to use the test system. *See*: "Travelers over the age of 14 and under 79 will be required to participate in the test," CBP Deploys Test of Departure Information Systems Technology at Hartsfield–Jackson Atlanta International Airport. June 13, 2016. Available at: https://www.cbp.gov/newsroom/local-media-release/cbp-deploys-test-departure-information-systems-technology-hartsfield. Regarding more recent notice, in 2017, CBP published a PIA, which few passengers would have read. CBP states that it put some signage up, but the signage does not guarantee proper legal notice to all passengers. See Appendix A. *See also:* US Department of Homeland Security, Privacy Impact Assessment, Privacy Impact Assessment Update for the Traveler Verification Service (TVS): CBP-TSA Technical Demonstration Phase II DHS/CBP/PIA-030(e) (August 14, 2018). Available at: https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030e-tvs-august2018_0.pdf.

[16] *Supra* note 15.

flow risks.

There may be compelling travel security justifications for implementing the program, but knowing if the proposed technology is actually going to work as promised requires public input and consultation. DHS must view the public comment process as a meaningful opportunity for consultation with the public, biometrics experts, academics, and researchers. Public comments will contribute value and help identify improvements in the functioning and security of the program.

The long history of biometric implementations around the globe[17] is rife with examples showing that policy needs proper assessment long before the implementation of biometric technology. We cannot emphasize this point enough. India's vast Aadhaar biometric ID ecosystem is a prime example, one which we researched in the field and subsequently wrote about in peer-reviewed research in *A Failure to Do No Harm: India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*[18] With India's Aadhaar implementation, biometric ID was supposed to solve India's identity problems. Instead, a government post-implementation report found that some states had high "failure to match" rates. The government research stated that "...estimates include 49% failure rates for Jharkhand ... and 37% for Rajasthan." The report stated that "Failure to identify genuine beneficiaries results in exclusion errors."[19] The biometrics hardened some of the existing problems and created new risks. Much of this could have been avoided had there been proper policy work done prior to implementation. DHS should expect some technology failures with the biometric entry and exit program. Prudence and public policy should compel DHS to seek the input, through formal notice and comment, of experts from the public so as to properly and fully anticipate problems and successfully mitigate for them.

Biometric systems have been implemented globally for decades, with some major implementations in the last decade. What we have learned from the problematic implementations is that they share something in common: biometric technology was put in place before adequate public consultation, without clearly articulating the problem the technology was going to solve, and without clearly identifying new risks created by the technology and fully mitigating those risks. This is a problem that DHS can move toward resolution with a comment period under the APA.

---

[17] John Emerson and Pam Dixon, National IDs Over Time, Infographic. World Privacy Forum, August 2017. Available at: https://www.worldprivacyforum.org/2017/08/national-ids-over-time/ . This infographic, based on World Bank's ID Unit data, shows ID systems from the 1800s through to 2017, of which a portion are biometric ID systems.

[18] *A Failure to Do No Harm: India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.* Pam Dixon, Springer Nature, *Health Technology*. DOI 10.1007/s12553-017-0202-6. Available at: http://rdcu.be/tsWv. Open Access via Harvard-Based *Technology Science*: https://techscience.org/a/2017082901/.

[19] *A Failure to Do No Harm: India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.* , Pam Dixon, Springer Nature, Health Technology. DOI 10.1007/s12553-017-0202-6. Available at: http://rdcu.be/tsWv. See p. 547. *See also*: National Economic Survey, India, 2016–2017, p, 202. Available at: http://indiabudget.gov.in/es2016-17/echapter.pdf.

IV. Ownership of cameras in airports, applicable laws, and data flow complexities

WPF met in-person with CBP, along with other NGOs, in San Francisco during January 2018.[20] CBP discussed the broad contours of this meeting in a press release.[21] At this meeting, the World Privacy Forum raised concerns regarding the issue of ownership of airport cameras and the data and privacy complexities the airport cameras create. We also raised concerns about secondary use of the biometric data by commercial entities such as airlines, and potentially other commercial entities. We requested that DHS pay attention to these issues. The new Privacy Impact Assessment (August, 2018) does not address the issues regarding airport cameras and data complexities. The new PIA admits secondary use by airlines is an unmitigated privacy risk.

Regarding the issues related to airport cameras, since the January meeting, we conducted additional research and can now unambiguously document that airports have a plethora of cameras under a variety of ownership structures, use different administrative and contractual controls, and are subject to widely differing policies and laws. Meanwhile, travelers have no idea what happens to their biometric data collected from cameras, who owns it, what rights (if any) they have, or what law applies to the use of those cameras or the images, video and sound they capture. Given the situation, no one can reasonably call traveler participation voluntary. The lack of due process here is stunning.

Just to emphasize the point here, we found that in US airports, there are:

- Cameras installed and operated by the airport;
- Cameras installed and operated by the Port Authority of the state;
- Cameras installed and operated by retailers and other commercial (non-governmental) entities;
- Cameras installed and operated by the airlines;
- Cameras installed and operated by TSA;
- Cameras installed and operated by Customs and Border Protection;
- Cameras installed and operated by other law enforcement personnel, (state or municipal).

Depending on the installer/operator, cameras may be:

- Subject to state law regarding privacy and document production / destruction requirements;

---

[20] Representatives from WPF and other privacy groups also attended, including EFF, which wrote a letter to CBP after the meeting. *See*: EFF Follow up letter to Customs and Border Protection, Electronic Frontier Foundation, February 15, 2018. Available at: https://www.eff.org/document/eff-follow-letter-us-customs-and-border-protection.

[21] US Department of Homeland Security, Customs and Border Protection, Press Release: Privacy meeting; CBP Meets with Privacy Groups to Discuss Biometric Exit, February 2, 2018. Available at: https://www.cbp.gov/newsroom/national-media-release/cbp-meets-privacy-groups-discuss-biometric-exit-0. Note regarding attendance: World Privacy Forum executive director Pam Dixon attended the CBP meeting in person in San Francisco.

- Subject to federal requirements and laws;
- Subject to Section 5 of the FTC Act;
- Subject to no specific laws.

Camera data/ video feeds may be:

- Stored and or used for general law enforcement purposes;
- Feeds may be shared between operators for federal or state purposes, including law enforcement (A camera installed by a port authority may be shared with the TSA, for example. In this instance, the feed could be subject to state and federal law.);
- Subject to FOIA requests, depending on the camera and applicable state and other laws and regulations;
- Used in criminal prosecution;
- Used in private litigation;
- Used by commercial entities for secondary purposes unrelated to identification.

Cameras in airports can be run under numerous different legal frameworks, with different rights attaching to the data feeds resulting from those cameras. It is unlikely that travelers would be privy to every right assigned to every camera.

For example, in the state of Oregon, cameras that are ***owned by the airport*** are subject to surveillance tape record retention schedules set under Oregon Administrative Rules, OAR 166 - 150 - 0135, subsection 76. This OAR sets minimum retention rules regarding video surveillance footage, for example.[22] This allows travelers to submit information requests for the feeds, and creates a prescribed document destruction period for the data, which is 30 days, unless exceptions apply. But ***cameras owned by the airlines*** and that are located in the very same airport are not subject to these rules. ***Cameras owned by CBP*** located in the same airport operate under yet a different set of rules.

To say that the cameras in airports create a nearly unknowable patchwork of laws and regulations understates the problem. We doubt that even the owners or operators of the cameras are aware of applicable laws and rules, and we doubt that anyone, anywhere has a compendium identifying the laws and rules applicable to each camera collecting images in airports. Indeed, if such a compendium exists, DHS ought to make that information available to the public.

The presence of entirely new cameras installed for the collection of biometrics and

[22] Oregon Administrative Rules, OAR 166 - 150 - 0135, Section 76. Available at: https://secure.sos.state.or.us/oard/viewSingleRule.action?ruleVrsnRsn=26067. (76): "Surveillance Tapes: Records documenting the routine monitoring of courts and other facilities through the use of video recordings. These recordings contain daily footage of activities in the courthouse or other county facilities and may also serve as evidence in criminal proceedings. (Minimum retention: (a) Retain tapes used as evidence: until case reaches final disposition (b) Retain tapes used for internal investigations: until investigation ends (c) Retain all other tapes: 30 days)."

related data collection only compounds the problems associated with this unruly data ecosystem and the failure to provide adequate public notice and opportunity for public comment.

We restate to DHS that the camera installation and ownership at each airport represents a complex and unruly data ecosystem. We urge DHS, working with port authorities, airlines, and airport landlords, to map all cameras at airports and determine with specificity who owns or controls each camera and what laws pertain to those cameras. DHS should also identify which data feeds are going where, and what, if any, protections for the traveling public apply with respect to the usage of the footage or sound captured by those cameras. Rules pertaining to data flows and cameras should be mapped to each camera to create a complete framework of permissions, rights, and data flows. There should be no surprises regarding data feeds from cameras in airports, and there should not be a single unmapped camera. This is good for privacy, and it is also good for security.

There should be no surprise cameras anywhere in any airport, and there should be a robust permissions and mapping process in place so that any camera placed in an airport has to be permissioned and mapped prior to installation.

Air travelers should know when state or federal laws apply to camera feeds, and have clear, prominent signage that documents rights they have in regards to the contents of those camera feeds. "Maps" of camera ownership and data flows need to be made available to the public.

V. Technical security risks with biometrics that are unaddressed in the PIA, including morphing risks

Major technical security issues exist regarding biometric systems such as biometric spoofing,[23] biometric template takeover,[24] and the fairly recent and increasingly well-documented challenges with biometric morphing[25] that are highly relevant to borders and passport control. These risks have not yet been addressed by DHS in its published PIAs.

Morphing attacks[26] in particular are a pernicious and unwanted threat to the biometric

---

[23] Anil K. Jain, Arun A. Ross, and Karthik Nandakumar. Introduction to Biometrics. Springer: New York, London. Chapter 7, Security of Biometric Systems. See pp. 269-278.

[24] Anil K. Jain, Karthik Nanakumar, and Abhishek Nagar**.** *Biometric Template Security*, EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics, January 2008. Available at: http://www.cse.msu.edu/~rossarun/BiometricsTextBook/Papers/Security/JainNandakumarNagar_TemplateSecuritySurvey_EURASIP08.pdf . *See also*:
Anil K. Jain, Arun A. Ross, and Karthik Nandakumar. Introduction to Biometrics. Springer: New York, London. Chapter 7, Security of Biometric Systems.

[25] U. Scherhag et al. A. Bromme, C. Busch, A. Dantcheva, C. Rathgeb and A. Uhl, Eds. Biometric Systems under Morphing Attacks: Assessment of Morphing Techniques and Vulnerability Reporting. BIOSIG 2017, Lecture Notes in Informatics (LNI), Gesellschaft fur Informatik, Bonn 2017. Available at: https://christoph-busch.de/files/Scherhag-Methodology-BIOSIG-2017.pdf.

[26] *Morphing* is a type of presentation attack where biometric samples (such as photographs) of multiple individuals are merged, typically using photographic editing software. The final merged image can be comprised of 2 or more photos. The goal of a morphing attack is to allow a successful biometric

entry and exit program, and this type of attack can also present a risk to individuals whose demographic data and/or images have been stolen and used as a contributing subject for a morphed ID, such as a passport.[27] NIST has begun its Facial Recognition Vendor Testing project focused on this issue, FRVT MORPH,[28] as of September 2018. The FRVT MORPH test will "provide ongoing independent testing of prototype facial morph detection technologies" and will "test both algorithmic capability to detect facial morphing (morphed/blended faces) in still photographs as well as face recognition algorithm resistance against morphing." The NIST project to research morphing is important, and one of the first major efforts in this area.

Is the biometric entry and exit program addressing morphing risks? If so, how? What morph detection system, if any, is the CBP system using? What procedures are in place to assist individuals who may have had their identities (demographic data and/or images) compromised without their knowledge? The department will benefit from addressing these challenges prior to implementation. Again, the chief privacy officer of DHS has full authority to identify these problems and to make sure that DHS components address them. Morphing, in particular, is a substantial risk that needs to be addressed.

VI. High 90th percentile accuracy in theory versus the actual reality of errors in a biometric installation

In its discussion of the biometric program implementation, CBP has issued a statement noting that its biometric program achieved accuracy at a high 90th percentile.[29] This may seem like a high number, unless and until you are the individual who is not authenticated by the program. Failures to enroll and authenticate are common in biometric systems. They are in fact much more common than DHS admits. NIST conducts robust and ongoing facial recognition vendor testing (FRVT). Even the briefest perusal of the NIST

---

verification of all contributing subjects against the final "morphed" identity. A high quality morphed image can be very difficult to detect. Morphing can occur in facial recognition or other biometrics systems. In this letter, we refer to morphing attacks on facial recognition systems. *See also:* International Organization for Standardization: Information Technology, Biometric presentation attack detection, Part 3: Testing and reporting. ISO/IEC FDIS 30107-3:2017, JTC 1/SC 37, Geneva, Switzerland, 2017.

[27] A robust discussion of passport morphing is available in: U. Scherhag et al. A. Bromme, C. Busch, A. Dantcheva, C. Rathgeb and A. Uhl, Eds. Biometric Systems under Morphing Attacks: Assessment of Morphing Techniques and Vulnerability Reporting. BIOSIG 2017, Lecture Notes in Informatics (LNI), Gesellschaft fur Informatik, Bonn 2017. Available at: https://christoph-busch.de/files/Scherhag-Methodology-BIOSIG-2017.pdf.

[28] Mei Ngan, Patrick Grother, and Kayee Hanaoka. Face Recognition Vendor Test MORPH Performance of Automated Facial Morph Detection and Morph Resistant Face Recognition Algorithms, Concept, Evaluation Plan and API, VERSION 1.1. NIST. Sept. 6, 2018. Available at: https://www.nist.gov/sites/default/files/documents/2018/09/07/frvt_morph_api_v1.1.pdf.

[29] Marcy Mason, US Customs and Border Protection, Biometric Breakthrough: How CBP is meeting its mandate and keeping America safe. Frontline, Vol. 9 Issue 3. Available at: https://www.cbp.gov/sites/default/files/assets/documents/2018-Jun/Frontline%20-%20Vol9%20Iss3%20-%20Web.pdf. Page 13: 'After more than a year of testing, the facial recognition technology has consistently shown a high rate of accuracy. “Our percent of successful matches is in the high 90s. It’s even moved up a notch in terms of quality and accuracy,” said Nael Samha, CBP’s director of passenger systems who built the architecture for the pilot’s operating system.'

test results reveal differences among algorithms, including differences in accuracy.[30] That accuracy and algorithms differ is not a disputed fact in the industry.

Is there a NIST vendor accuracy test for all of the systems being used by CBP for facial recognition?[31] If DHS is going to use facial recognition technology, and allow airlines to use biometric technology on its behalf, then all of the biometric technology used by all participating parties should be required to undergo NIST testing so that the public knows what error rates the technology has. Each member of the traveling public who has their biometrics collected and analyzed should be told:

- What company produced the algorithm(s),
- What biometric system(s) is/are in use, and
- Be pointed to the NIST test of that/those system(s).

Biometric accuracy is now a well-studied area of inquiry. Research documents that when inaccuracies in biometric systems occur at scale, scale effects occur and create non-trivial challenges.[32] Large numbers of passengers screened daily, for example, at a 98% accuracy level means that with an approximate 2% error rate, there could be 20,000 potential failures for every one million passengers screened. This is an oversimplification of the problem, because there are different types of failures, and a number of complex variables can shift outcome numbers. But it makes the point. Does DHS have the capability of handling meaningful numbers of enrollment failures, failures to authenticate, false positives, or false negatives each day in the midst of high-stress, time-is-of-the-essence, round-the-clock airport operations? Moreover, what are the consequences to those would-be travelers who are wrongly flagged or otherwise experience difficulties related to the biometric system? What redress do they have, if any? What happens to passengers whose image has been used in a morphed ID, unbeknownst to them?

In the CBP system, the impact of errors could range from missing a flight, to much more serious impacts for people with false positives who are identified as non-citizens, false positives as a potential subjects for law enforcement investigation, or a false negative for a person who really did pose a safety threat. Those who are subject to failures to enroll or authenticate can include groups of individuals to which increased biometric bias applies, something that is well-researched and documented, and this effect is well-documented in

[30] https://www.nist.gov/sites/default/files/documents/2018/06/21/frvt_report_2018_06_21.pdf
[31] The CBP biometric entry and exit systems use NEC as at least one of its vendors. See: NEC Press Release: NEC tests facial recognition with U.S. Customs and Border Protection (CBP) on select Dulles International Airport (IAD) flights. NEC, June 27, 2018. Available at: https://www.nec.com/en/press/201706/global_20170627_03.html.
[32] Brian DeCann and Arun Ross, De-Duplication Errors in a Biometric System: An Investigative Study. Proc. of IEEE International Workshop on Information Forensics and Security (WIFS), (Guangzhou, China), November 2013. Available at: https://www.cse.msu.edu/~rossarun/pubs/DeCannRossDeDuplicationError_WIFS2013.pdf .

the border/passport context.[33] For example, an ISO technical report recommendation for the Canadian Temporary Resident Biometric Project was that children older than 5 may be able to use facial recognition, but "the false reject rate will be significantly higher than for adults. All children can still provide a facial image for human verification (although humans also perform poorly at facial recognition for children) but automated facial recognition is not recommended." Many other considerations exist regarding age, gender, and other biases.

VIII. Sharing of airline travel test data with commercial entities

We are deeply concerned about the sharing of biometric data with commercial retailers within the airport, for example, duty free shops. The public must also be clearly informed as to the role of the airlines in this program. In the DHS Privacy Impact Assessments, DHS admits that an unmitigated privacy risk exists in the biometric entry and exit system, specifically, that airlines can use the biometric data for unrelated, secondary purposes -- purposes entirely unconnected to the CBP program or even identifying passengers for safety purposes.[34] CBP claims it cannot control the airlines' secondary use of the data, nor retention times, just make suggestions. CBP officials envision airports that contain a "biometric pathway" across the airport, presumably in a variety of commercial settings.[35] Our concerns regarding data privacy of travelers are not assuaged by the statements of CBP regarding airline handling of the data, nor are we assured by the statements of the airlines in regards to the carriers' handling of the data.

If travelers want to participate in biometric payments as a separate data flow originating with a commercial retailer, in a fully voluntary program separated from identification for travel purposes, that is one thing. But to give what are essentially non-voluntary

---

[33] Dr. John W. M. Campbell. ISO Technical Report, (ISO/IEC JTC-1 SC 37). Demographic Bias in Biometric Systems: Current Research and Applicable Standards, January 2017. Available at: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc265/p805126_A1b.pdf.

[34] US Department of Homeland Security, Privacy Impact Assessment, Traveler Verification Service (TVS): Partner Process DHS/CBP/PIA-030(c) June 12, 2017. Available at: https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-june2017.pdf**.** From the PIA: "Privacy Risk: There is a risk that approved partners will use biometric images collected under the TVS for a purpose other than identity verification. Mitigation: This risk cannot be fully mitigated. Under the TVS-partners initiative, industry partners collect photographs consistent with their contractual relationships with the travelers and voluntarily provide them to CBP in support of this project. The original collection is subject to the contract between the industry partner and the traveler, to which CBP is not a party."

[35] Russell Brandom, A Biometric Pathway Through the Airport, Unlocked by your Face. The Verge, May 9, 2017. Available at: https://www.theverge.com/2017/5/9/15591648/airport-facial-recognition-customs-tsa-biometric-exit. From the article: 'Led by Customs and Border Protection, the plan is built around the Biometric Exit program, which will register visitors leaving the US using facial recognition. But new statements show that CBP's plans could make facial scans necessary for US citizens as well, documenting them when they reenter the country or pass through TSA checkpoints. The result would eventually grow into an airport-wide system Customs officials call "The Biometric Pathway." John Wagner, deputy assistant commissioner at CBP, laid out that vision at the ConnectID conference last week. "We're going to build this for [Biometric] Exit. We're out of time, we have to," Wagner told the crowd. "But why not make this available to everyone? Why not look to drive the innovation across the entire airport experience?"'

biometric captures to commercial entities, or to use such biometric captures for secondary purposes unrelated to original CBP purposes, is a major misstep by the US government, and sets a terrible precedent for unfettered use of information collected in what are essentially mandatory settings. Indeed, given recent Congressional interest in consumer privacy issues, the exposure of biometric data of tens of millions of US persons to private companies due to CBP's program should be discussed by legislators who are armed with the facts of this collection and dissemination. We expect that Congress would find such a commercial dissemination without planning, limitation or redress violative of consumers' expectations while traveling.

We also observe that no existing federal privacy laws applies to all entities in an airport that might obtain passenger biometric data. Some state privacy laws may apply to some of the entities, but not to all of them. Because of the blend of applicable laws, the legal framework is likely to be different in every airport. The possibility of international sharing of passenger information with foreign governments or with foreign corporations raises an additional welter of privacy and compliance issues.

We observe that the legal issues raised by the sharing of personal data collected by DHS for security and identification reasons with commercial enterprises are so complex that merely outlining the issues would make a wonderful question for a four-hour law school exam.

IX. The Biometric entry and exit program and the Violence Against Women Act

Congress has repeatedly shown great concern for the safety of victims of domestic violence, stalking, abuse, human trafficking, and other crimes against women and children. The strong and consistent congressional support for the Violence Against Women Act (VAWA), including those actions directly impacting applicability of VAWA to DHS activities, is a testament to that concern. Several provisions of VAWA apply directly and indirectly to DHS, and it is incumbent on DHS to explore its statutory obligations and to do so in consultation with representatives of the domestic violence community.

It is our analysis that the biometric entry and exit pilot program violates VAWA in letter and in spirit. DHS is installing a broad, and now greatly expanded Phase II pilot without careful analysis of VAWA applicability. In the first Privacy Impact Assessment, there was no risk analysis regarding VAWA, or women and children victims or survivors of domestic abuse and crime. In CBP's second PIA, published in August 2018, it also left out any risk analysis regarding VAWA or women and children victims and survivors. The omission of a VAWA risk analysis and mitigation is an error that can negatively impact the safety of potentially 1 in every 4 women in the United States.

US law makes it the responsibility of DHS to conduct a detailed and expert analysis of the biometric entry and exit program in relationship to VAWA, to assess the risks to victims of domestic violence, to publish that assessment in a risk assessment, and to fully comply with VAWA. In our analysis of the system, from what we can see from the

outside, we readily found multiple applicable provisions that create direct responsibility for compliance. We have not included all of the applicable provisions here, but there is much more for DHS to do. DHS needs to present its analysis of its VAWA obligations publicly.

X. Conclusion and request for immediate APA notice and comment period and compliance with VAWA

In closing, thus far, CBP's responses to criticisms and concerns about its biometric entry and exit program fail to respect applicable laws, regulations and prudent public policy.[36] DHS signage is inadequate to provide meaningful notice.[37] The program has expanded beyond the pilot stage and is close to full implementation. Plus, DHS faces legal liability in its non-compliance with both the APA and potentially VAWA. Further, it has underestimated or at least not made clear to the public in its PIAs the risks of complex data flows, and the risks of biometrics systems, including technical security risks.

We request that DHS immediately:

1. Undertake a full notice and comment period for this program under the APA; and
2. Address how biometric entry and exit will specifically comply with VAWA.

Further, we request that DHS share the following information publicly:

1. The name(s) of the biometric vendors in use (including pilot program use) for all airlines, CBP, and TSA;
2. The NIST facial recognition vendor tests for all biometric vendors involved in the pilot project;
3. If vendors did not submit their facial recognition algorithm to the NIST FRVT, do the vendors plan on submitting their algorithms for the NIST biometric vendor tests, and when;
4. If a NIST biometric vendor test does not exist for the relevant vendor(s) we request the vendors' self-test to be made public;
5. What morph detection mitigations, if any, has the CBP system has employed, including for affected individuals who may be ID theft victims;
6. A complete list of all airports and other border crossings (sea and land) participating in the biometric program as of September 18, 2018; and
7. Copies of the Memoranda of Understanding between CBP, the airlines, other transportation companies and other entities participating in the pilot program, including biometric systems vendors.

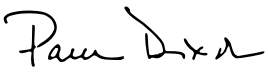
[36] Statement by CBP to International Business Times. As quoted in: Denisse Moreno, Facial Recognition Failure? DHS Passenger Face Scanning Program Expansion Should Stop, Senators Say. International Business Times, Dec. 21, 2017. Available at: https://www.ibtimes.com/facial-recognition-failure-dhs-passenger-face-scanning-program-expansion-should-stop-2631616.

[37] See Appendix A for a screenshot of the DHS biometric entry and exit signage.

The problems that the biometric entry and exit program faces are serious. They are likely to prevent DHS from achieving its goals in any fair or effective way. Yet, while our concerns focus on privacy and related consequences, we do accept that the broad objectives that DHS seeks to achieve have a reasonable basis in law. Finding a better way to involve all the relevant stakeholders in this situation will bring DHS into compliance with applicable statutes and it will also enable DHS to succeed in making its program work on its own terms.

We do not seek to throw a wrench into the process just to stall action. Rather, our objective is to find a better way to achieve compliance with the multiple legal obligations and policy goals that DHS seeks to achieve. All of us want safe air travel. The World Privacy Forum and others are willing and able to help DHS, but DHS must take the next step by seeking to engage us and the broader public in some way. Establishing a meaningful notice-and-comment process under the APA is a good way to begin. Should you have questions or would like to discuss these issues further, please do not hesitate to contact me at 760-470-2000.

Sincerely,



Pam Dixon,
Executive Director,
World Privacy Forum
www.worldprivacyforum.org

Appendix A: Screenshot of DHS Sample biometric entry and exit signage

Figure 1, below, is a screenshot of DHS signage regarding the biometric entry and exit program. The sign:

- Does not indicate the voluntariness of the program;
- Does not indicate a specific, dedicated DHS biometric entry and exit page for immediately and directly accessing relevant information; and
- Does not inform travelers that they can make FOIA requests regarding their biometric data, nor where precisely to find that information.

The Department of Homeland Security published this sample signage seen in Figure 1 below in its Privacy Impact Assessment update DHS/CBP/PIA-030(c), available at: https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-june2017.pdf. The sample signage is available on p. 17 of the PIA.

Other signs may be available, however, we are relying on the information published in the Privacy Impact Assessment update, DHS/CBP/PIA-030(c).

Homeland Security

Privacy Impact Assessment Update
DHS/CBP/PIA-030(c) TVS: Partner Process
Page 17

APPENDIX A: Sample Sign with Privacy Notice

Posted at Airport Departure Gates

(near Partner-Operated Cameras):

[CBP Partner] is collecting facial images and sharing them with CBP to verify each traveler's identity and to create a record of departure from the United States. For more information, please visit our website at www.cbp.gov.

Figure 1: Screenshot of p. 17 of DHS Privacy Impact Assessment update *DHS/CBP/PIA-030(c), available at:* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-june2017.pdf

Appendix B: All airports participating in biometric air exit and entry

The source for this data is Customs and Border Protection, https://www.cbp.gov/travel/biometrics, as of September 18, 2018.

Biometric Air Exit and Air Entry

	Air Exit - US Airports	Air Entry - US Airports
	Atlanta ATL	Atlanta ATL
	Boston BOS	
	Chicago O' Hare ORD	
	Detroit DTW	
	Dulles IAD	
	Houston Hobby HOU	
	Houston Intercontinental IAH	Houston Intercontinental IAH
	John F. Kennedy JFK	JFK
	Las Vegas LAS	
	Los Angeles LAX	Los Angeles / Tom Bradley (TBIT)
	Miami MIA	Miami MIA
	Orlando MCO	Orlando MCO
		San Jose (SJC)
		San Diego SAN
	San Francisco SFO	
	Seattle SEA	
		Air Entry - Overseas Airports
		Abu Dhabi Preclearance AUH
		Aruba Preclearance AUA
		Dublin Preclearance DUB
		Shannon Preclearance SNN

Figure 2: Airports participating in biometric entry and exit as of September 18, 2018.