Privacy Impact Assessment Update
for the
1-to-1 Facial Comparison Project

DHS/CBP/PIA-025(b)

October 18, 2016

Contact Point

Kim A. Mills
Director
Entry/Exit Transformation Office
Office of Field Operations
U.S. Customs and Border Protection
(202) 344-1076

Reviewing Official

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

U.S. Customs and Border Protection (CBP) is updating the Privacy Impact Assessment (PIA) for the 1-to-1 Facial Comparison Project due to a change in the retention of facial images of travelers presenting themselves at the border for customs and immigration inspection. CBP uses facial comparison technology to assist CBP Officers in determining whether an individual presenting a valid electronic passport, or "e-Passport," is the true owner of that document. This PIA update documents CBP's change in procedures to retain select facial images taken during primary inspection and all facial images taken during secondary inspection.

Overview

In March 2015, CBP published the original 1-to-1 Facial Comparison Project PIA[1] to notify the public of a new pilot to test the use of facial comparison technology to assist in identifying fraudulent use of valid U.S. passports. The pilot was deployed at select airports with two main goals: (1) to assess the impact of the technology on the customs and immigration inspection process and ensure it could be deployed with minimal delays and impacts on travelers; and (2) to test an image matching algorithm and identify the optimal parameters to maximize match confidence and minimize the risk of errors. CBP conducted the pilot over a 19-month period, from laboratory testing to analysis. Live testing at airports was conducted with U.S. e-Passport holders at random and was limited to a 60-day period from March 2015 to May 2015. Based on the results of the pilot, CBP deployed the facial comparison project in 2016 to additional air ports of entry and expanded the program to include first-time Visa Waiver Program travelers; CBP published a PIA update[2] documenting this implementation in January 2016.

CBP uses facial comparison technology at various stages in the immigration inspection process. When individuals first present themselves to CBP Officers for customs and immigration inspection (known as "primary inspection" or "primary"), CBP Officers may take a photo of the individual and use facial comparison software to compare it against the photograph contained in the e-Passport's chip.[3] The software generates a match score indicating the likelihood that the individual pictured in the e-chip photograph is the same individual presenting the document. If a low match confidence score results, the CBP Officer refers the individual for further inspection (known as "secondary inspection" or "secondary"). CBP Officers conducting secondary inspections retake the photo for facial comparison purposes; if an enforcement action is taken, this photo will be retained with other information in the case file.

---

[1] *See* DHS/CBP/PIA-025 1:1 Facial Recognition Air Entry Pilot, March 11, 2015, *available at* www.dhs.gov/privacy.
[2] *See* DHS/CBP/PIA-025(a) 1:1 Facial Comparison Project, January 14, 2016, *available at* www.dhs.gov/privacy.
[3] In 2007, the U.S. Department of State embedded a computer chip in all newly issued U.S. passports (known as electronic passports or "e-passports,") as part of an overall effort to prevent imposters from using valid U.S. passports to enter the country.

Reason for the PIA Update

CBP is issuing this PIA update to provide notice that it is expanding retention of photos to include facial images taken during primary inspection with scores that fall in the mandatory referral range, as well as all photos taken during secondary inspection. At the outset, CBP only retained facial images taken during secondary inspection that were linked to a law enforcement or administrative action. Over the course of the program's implementation, CBP has recognized that continuous assessment of the facial comparison software requires a test set of photos for these purposes. To address this gap, CBP plans to retain select facial images taken during primary inspection and all photos taken during secondary inspection. These photos will be retained for testing and administrative purposes, including quality assurance evaluation, data analysis, and internal affairs review. If an individual was not referred to secondary inspection, any facial image retained from primary inspection will be used solely for testing and quality assurance purposes (and internal affairs, if necessary). CBP will continue to retain all facial images taken during secondary inspection processing for law enforcement or administrative action.

CBP's retention of traveler photos from both primary and secondary inspections enables a thorough review of its facial comparison technology. CBP may assess several factors to ensure the accuracy of the facial comparison software, including:

1) What may account for a low match comparison score at primary if secondary inspection indicates that the traveler is using his or her own valid passport;
2) Whether environmental or technical factors may cause primary and secondary scores to vary substantially; and
3) Where CBP should set the lowest acceptable match comparison score, below which referral for secondary inspection is mandatory.

CBP is expanding the retention of facial images under this project to include certain photos from primary inspection because they are valuable to CBP's assessment of the accuracy and value of the facial matching technology.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal Government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of PII. The Homeland Security Act of 2002

Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act.[4]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure the United States.

DHS conducts PIAs on both programs and information technology systems, pursuant to Section 208 of the E-Government Act of 2002 and Section 222 of the Homeland Security Act of 2002. CBP conducted this FIPPs-based PIA because the 1-to-1 Facial Comparison Project collects privacy sensitive information but does not use an information technology system as defined in the E-Government Act. This PIA examines the privacy impact of 1-to-1 Facial Comparison Project operations as it relates to the FIPPs.

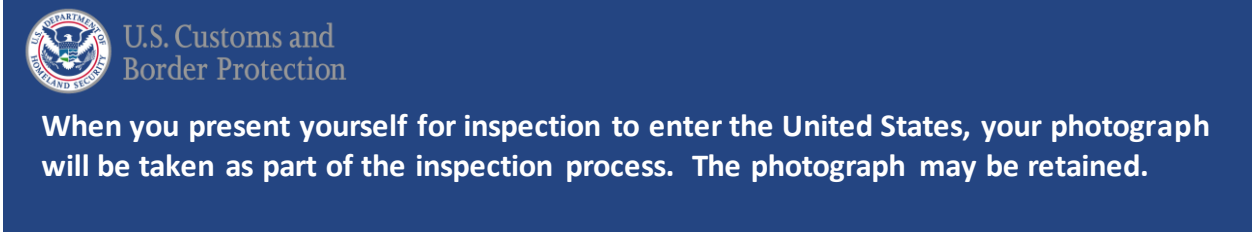
1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

CBP is updating this PIA to inform the public that the 1-to-1 Facial Comparison Project is now retaining all facial images taken during secondary inspection, and certain facial images taken during primary inspection. For images from primary inspection, CBP will retain any images with scores that fall in the mandatory referral range. CBP will retain these images for quality assurance evaluation, data analysis, and internal affairs review.

There are no new risks to notice since the last PIA update. As described in the original 1-to-1 Facial Comparison Project PIA, CBP is providing transparency to the public about this pilot by posting signage in close proximity to facial recognition cameras at each testing site to inform the public that CBP is taking a photograph of U.S. e-passport holders. The original signage also stated that facial images are not retained or used outside of the Department of Homeland Security. CBP updated the signage in January 2016 to notify the public that CBP may retain secondary inspection photographs. The signage will remain the same for the limited expansion to primary inspections (see figure below).

[4] 6 U.S.C. § 142.



CBP is updating this PIA to provide notice to the public that photos taken during primary inspection also may be retained if scores fall within the mandatory referral range, however these photographs are used for testing purposes only and are not linked to an individual's border crossing record. For photographs retained from secondary inspection, any information that becomes associated with an enforcement record for that traveler becomes part of that case file consistent with the TECS System of Records Notice (SORN). [5]

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

No change has occurred to individual participation since the last January 2016 PIA. The original privacy risks remain.

Privacy risk: There is a risk that individuals will be falsely identified as imposters as a result of the facial comparison score and will not have the ability to correct this assessment.

Mitigation: This risk is mitigated by the fact that CBP does not rely on facial comparison technology alone to identify fraudulent use of a valid passport. During additional screening, the CBP Officer interviews the traveler, who is provided the opportunity to present other forms of identification or provide additional information (for example, confirm details of his/her travel history) as further evidence of his/her identity.

Persons, who believe they have been improperly denied entry, refused boarding for transportation, or identified for additional screening by CBP, may submit a redress request through DHS Traveler Redress Inquiry Program (TRIP). DHS TRIP is a single point of contact for persons who have inquiries or seek resolution regarding difficulties they experienced during their travel

[5] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, December 19, 2008, *available at* www.dhs.gov/privacy

screening at transportation hubs – like airports, seaports, and train stations or at U.S. land borders. Through DHS TRIP, a traveler can request correction of erroneous data stored in DHS databases through one application. DHS TRIP redress requests can be made online at https://www.dhs.gov/dhs-trip or by mail at:

DHS TRIP
601 South 12th Street, TSA-901
Arlington, VA 20598-6901

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

No change has occurred to the overall purpose and authorities of this program[6] since the January 2016 PIA. While the scope of the project has expanded, it remains consistent with the original authorities and purpose of collection. CBP has clearly articulated the specified purpose and authority for this collection of PII.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

During the initial pilot, retention of collected facial images and facial match score data was limited to the duration of the pilot (nineteen months) and used primarily to evaluate the technology. When the project became operational, photo retention was limited to facial images taken during secondary inspection if the inspection resulted in a law enforcement or administrative action. However, this restricted retention limited CBP's ability to conduct quality assurance evaluations, data analysis, and internal affairs reviews. To meet this administrative need, CBP will retain all facial images taken during secondary inspection and in primary inspection when facial comparison scores fall in the mandatory referral range. CBP will use only photos and non-PII data to evaluate system performance and to report operational metrics. This non-PII data is limited to comparison match scores, number of travelers processed, and number of travelers referred to secondary. Photos retained for these administrative purposes will be disposed of after five years. Any information

[6] *See* 8 CFR 235.1(b); and 8 U.S.C. §1185(b) and (c).

associated with an enforcement record for an individual traveler will be retained by CBP and maintained for the life of the enforcement record, consistent with the TECS SORN.[7]

Privacy risk: There is a new risk of over-collection since CBP is now retaining photos from primary inspection for testing and administrative purposes

Mitigation: This risk is partially mitigated. The increased retention of data is limited to photos and non-PII, and used to evaluate system performance and provide metrics for reporting purposes. Photos retained for this purpose will be retained for five years and will only be stored with non-personally identifiable data. CBP's retention of all secondary facial images and primary facial images scoring in the mandatory referral range represents only a moderate increase in overall photos retained and will improve the effectiveness of the tool. However as before, any information that becomes associated with an enforcement record for that traveler becomes part of that record consistent with the TECS SORN.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

There is no change from the January 2016 PIA. Although CBP is retaining additional photos, the use of these photos for testing and quality control of facial comparison software is consistent with the original purpose of the 1-to-1 Facial Comparison Project, which was in part to determine the validity of the technology and algorithm.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

No change from January 2016 PIA.

[7] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, December 19, 2008, *available at* www.dhs.gov/privacy

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

No change from January 2016 PIA.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

No change from January 2016 PIA.

Responsible Official

Kim A. Mills
Director
Entry/Exit Transformation Office
Office of Field Operations
U.S. Customs and Border Protection
202-344-1076

Debra L. Danisek
Acting CBP Privacy Officer
U.S. Customs and Border Protection
202-344-1610

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security