Privacy Impact Assessment Update
for the

1-to-1 Facial Comparison Project (formerly known as the 1:1 Facial Recognition Air Entry Pilot)

DHS/CBP/PIA-025(a)

January 14, 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
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

U.S. Customs and Border Protection (CBP) is expanding the 1-to-1 Facial Comparison Project (previously called the "1:1 Facial Air Entry Pilot") to operations in all U.S. air ports of entry and expanding the in-scope population to first-time travelers from Visa Waiver Program countries. The use of facial comparison technology assists CBP Officers (CBPO) in determining whether an individual presenting a valid electronic passport (e-Passport) is the individual pictured on the passport. CBP is updating this Privacy Impact Assessment (PIA) because the 1-to-1 Facial Comparison Project collects personally identifiable information (PII) in the form of facial images of travelers to assist CBPOs in making admissibility determinations.

Introduction

U.S. Customs and Border Protection's (CBP) primary mission is to protect the nation from terrorism and to foster economic security through lawful international trade and travel. CBP first conducted the 1-to-1 Facial Comparison Project using facial comparison technology use in 2015 to assist CBP Officers (CBPO) in identifying the possible fraudulent usage of valid passports.

In 2007, the U.S. Department of State (DOS) began embedding 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 United States. An e-Passport has a small integrated circuit (or "chip") embedded in the back cover with additional anti-fraud and security features. The chip securely stores: 1) the same information visually displayed on the photo page of the passport; 2) a biometric identifier in the form of a digital image of the passport photograph, which facilitates the use of facial comparison technology at ports of entry; 3) the unique chip identification number; and 4) a digital signature to protect the stored data from alteration.

Primary Inspection Processing

As described in the original PIA for the 1:1 Facial Air Entry Pilot,[1] when a traveler presents themselves for primary inspection at a booth equipped with facial comparison technology, the CBPO takes a photograph of the person presenting the e-Passport and compares it to the image contained in the e-Passport chip using the facial comparison system. The software

[1] For more information about the initial field test please see the DHS/CBP/PIA-025 1:1 Facial Recognition Air Entry Pilot PIA, available at, http://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-1-to-1-facial-recognition-20150311.pdf.

generates a match confidence score (scale 0-100) indicating the likelihood of a match between the two photographs.

Any U.S. citizen with an e-Passport arriving at a port that is participating in this project may be selected for facial comparison matching at port discretion.[2] Travelers presenting themselves for inspection at booths equipped with facial comparison technology do not have the option to opt-out of this process. The facial comparison system assists CBPOs in the inspection process but does not replace officer discretion at any point within the inspection process.[3] Facial images taken in primary inspection lanes during the entry process are not retained. The facial comparison project is another tool for CBPOs to use in conjunction with their normal policies and procedures. In secondary inspection, travelers will be asked additional questions and/or asked for additional documentation to verify their identity.

Secondary Inspection Processing

If referred, CBP conducts additional questioning and inspection processing (known as "secondary inspection" or "secondary") to determine if the person is an imposter, which may include retaking the facial comparison photo(s). The photo(s) taken will not be retained if the inspection does not result in an enforcement or administrative action (an action that negatively impacts a traveler's ability to enter the United States in a lawful status).

If the officer determines that an adverse action is warranted then a formal investigation begins. All records, including any photographs and score data, pertaining to an adverse action are maintained by CBP in TECS.[4] In this situation, the photos and score data taken during the secondary inspection are retained as part of the case file and then transferred via an encrypted and secure protocol to a secure database at the CBP National Data Center One (NDC1).

CBP may take another facial image of the individual in secondary to verify the person's identity. All facial image data that results from an adverse or law enforcement action in secondary inspection is retained per established CBP recordkeeping requirements. CBPOs are not permitted to manipulate, alter, erase, reuse, modify, or tamper with any facial image data. CBP takes precautions to prevent the alteration or deletion of the facial image data to ensure that all information is accurately captured and retained. The facial image data is only stored on a

[2] Supervisory CBPOs at each air port of entry participating in the project will set the standard for the random selection criteria and have discretion to change the criteria as needed.
[3] A person claiming U.S. citizenship must establish that fact *to the examining [CBP] officer's satisfaction* [emphasis added] and must present a U.S. passport or alternative documentation as required by 22 CFR part 53. If such applicant for admission fails to satisfy the examining immigration officer that he or she is a U.S. citizen, he or she shall thereafter be inspected as an alien. *See* 8 CFR 235.1. A U.S. citizen must present a valid unexpired U.S. passport upon entering the United States, unless he or she presents an excepted document. For additional information, *see* 8 CFR 253.1(b).
[4] DHS/CBP-011 U.S. Customs and Border Protection TECS (December 19, 2008 73 FR 77778).

CBP-approved server, which is only accessible by authorized CBP users. The facial image data is prohibited from being downloaded, manipulated, or otherwise used for personal use.

Access to the facial image data requires a login and user account password. CBP limits real-time access to the images and limits information displayed in the system from the e-Passport to the CBPOs conducting the specific inspection. Officers designated by the port will be provided access to pull adverse action reports (which only contain the photo image and comparison score data) directly from the secure database. These reports are appended to the case file which provides the evidentiary information that CBP may use in prosecuting a case. For a case dealing with a possible imposter, the case file would include the facial comparison matching procedures and score results that led the CBPO to determine that an individual is an imposter.

Reason for the PIA Update

CBP conducted a field test of 1-to-1 facial comparison technology at Washington Dulles International Airport (IAD) from March 2015 to May 2015.[5] During the field test, CBPOs took photographs of U.S. e-Passport holders during CBP arrival processing and then used facial comparison technology to compare the new image with the image stored on the e-Passport chip. CBPOs used the facial comparison technology as further evidence of identity verification along with existing entry procedures. Facial comparison software provided the CBPO with a match confidence score after the e-Passport chip was scanned and photo taken. The confidence score generated by the system was designed to detect possible imposters. Traveler photos taken during the pilot at IAD were retained in a stand-alone database to support project analysis and improve facial comparison capabilities.

CBP is updating the existing PIA because CBP is deploying this capability on a permanent basis to U.S. air ports of entry, expanding the scope of affected individuals to include first-time Visa Waiver Program (VWP) travelers, and changing the retention requirements.

Pilot Expansion

Since the last PIA was published in March, 2015, CBP has expanded the time-limited pilot to an indefinite project based on a rigorous evaluation of the project's technical and operational performance. The March 2015 test of this capability showed that biometric facial matching could increase the confidence with which CBPOs identified individuals without having a negative impact to port operations and traveler wait times. This is documented in a

[5] For more information about the initial field test please see the DHS/CBP/PIA-025 1:1 Facial Recognition Air Entry Pilot PIA, available at, http://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-1-to-1-facial-recognition-20150311.pdf.

comprehensive pilot report that included analysis of the impact to arrival processing operations, comparison of the performance of multiple facial comparison algorithms, and an assessment of appropriate scoring thresholds to ensure that only possible imposters were referred for additional inspection.

In this expansion, facial images taken in primary inspection lanes during the entry process will no longer be retained unless the traveler is subject to enforcement or administrative actions. The previous pilot program saved images for a short amount of time to conduct testing of the validity of the technology. Now, CBP will only retain facial images if a traveler is referred for additional inspection processing that results in a law enforcement or administrative action, at which point the images will be considered part of the case file and covered by the TECS SORN.[6]

CBP will begin an incremental deployment of facial comparison starting at John F. Kennedy International Airport (JFK) in January 2016. There is no end date to the deployments. The in-scope population will include returning U.S. citizens and first-time VWP travelers 18 and older. Returning U.S. citizens were identified in the last PIA.[7]

Expansion of In-Scope Population

The in-scope population is the same population of individuals as identified in the last PIA[8] with the addition of first-time VWP[9] travelers. During the initial field test at IAD, the in-scope traveler population only consisted of U.S. citizens (ages 18 and older) who presented e-Passports. CBP is expanding application of this technology to include first-time travelers from VWP countries ages 18 and above because DHS has identified an appreciable risk of passport and identity fraud among this population of travelers.

The VWP currently enables eligible nationals of 38 designated countries to travel to the United States for tourism or business purposes for stays of 90 days or less without first obtaining a visa.[10] VWP travel accounts for about two-thirds of all business and leisure travel to the United States. CBP currently uses fingerprints to biometrically enroll and verify VWP travelers' identity. Upon a VWP traveler's first visit to the United States, all ten fingerprints are collected and enrolled into the Department of Homeland Security (DHS) biometric database (IDENT).[11]

---

[6] DHS/CBP-011 U.S. Customs and Border Protection TECS (December 19, 2008 73 FR 77778).
[7] For more information about the initial field test please see the DHS/CBP/PIA-025 1:1 Facial Recognition Air Entry Pilot PIA, available at, http://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-1-to-1-facial-recognition-20150311.pdf.
[8] *Id.*
[9] http://travel.state.gov/content/visas/english/visit/visa-waiver-program.html#reference.
[10] http://travel.state.gov/content/visas/english/visit/visa-waiver-program.html.
[11] For more information about IDENT please see the DHS/NPPD/USVISIT/PIA-002, *available at,* http://www.dhs.gov/sites/default/files/publications/privacmory/PIAs/privacy_pia_usvisit_ident_appendixj_jan2013.pdf.

On subsequent visits, four fingerprints (index to little finger on one hand) are used to verify the individual against the fingerprints already in IDENT. Visitors seeking entry on a U.S. visa have already had all ten fingerprints enrolled into IDENT as part of their visa application process. For all entries into the United States, U.S. visa holders have their identity biometrically verified. CBP cannot biometrically verify the identity of a VWP traveler (on first arrival) as CBP can with visa travelers because VWP travelers do not require a U.S. visa and thus, have not been enrolled into IDENT prior to their first arrival to the United States. Thus, the 1-to-1 Facial Comparison Project allows CBP to biometrically match a VWP traveler to their e-Passport before enrolling that individual into DHS data systems. The 1-to-1 Facial Comparison Project provides CBP with a comparable level of confidence in verifying identities of travelers entering as a first-time VWP visitor, a VWP returning visitor, or a traveler entering on U.S. visa.

Retention of Images for Adverse Actions

CBP previously only retained the traveler's facial image and facial match score data during the field test, as detailed in the prior PIA. However, retention of this data included all travelers who were participants in the field test. In the expansion of this project, CBP will only retain facial images and comparison match score data from those travelers who are subject to an adverse or law enforcement action resulting from secondary inspection. All other facial images are not stored. CBP only maintains non-PII data to evaluate system performance and to report operational metrics. This data is limited to comparison match scores, number of travelers processed, and number of travelers referred to secondary.

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.[12]

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.

[12] 6 U.S.C. § 142.

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 general public that the 1-to-1 Facial Comparison Project is now being conducted indefinitely at U.S. air ports of entry. This is a change from the previous PIA, which only allowed collection from U.S. citizens for the two-month pilot period. CBP is updating this PIA and posting appropriate signage at the inspection booths at both air ports of entry that CBP is collecting facial images and that these images are retained if a law enforcement or administrative action occurs. Any information CBP retains will be associated with a case file for that individual traveler and covered by the TECS SORN.[13]

Privacy risk: CBP is updating this PIA and signage at all affected air ports of entry. There is no privacy risk to notice or transparency.

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.

The FIPPs principle of individual participation is not always practical or possible for this project due to CBP's law enforcement and other national security missions. Specifically, individuals are not able to "opt-out" or "opt-in" to this process. CBP is authorized to collect biometric information from applicants for admission into the United States claiming to be U.S. citizens and VWP travelers entering the United States. The authority to collect biometric data

[13] DHS/CBP-011 U.S. Customs and Border Protection TECS (December 19, 2008 73 FR 77778).

from VWP travelers is covered in several regulatory notices under United States Visitor and Immigrant Status Indicator Technology (US-VISIT).

Generally, all arriving applicants for admission must be inspected and admitted into the United States by CBP at an official port of entry. CBPOs must be able to request additional information to substantiate claims of U.S. citizenship because possession of a U.S. passport does not by itself constitute irrefutable evidence that a person seeking entry is a U.S. citizen.[8] Requiring CBP to obtain an individual's consent prior to the collection, use, dissemination, and maintenance of these photos would compromise enforcement operations, and would interfere with the U.S. government's ability to identify possible imposters attempting to enter into the U.S. and to protect its borders, thereby lessening the overall security of the United States. For these reasons, CBP is provided with broad authorities to inspect and search individuals as they enter the United States from abroad.[9][14]

Privacy risk: Individuals cannot opt-out of the 1:1 Facial Comparison Project.

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.

The authorities and purpose for this program remain the same.[15] In the interest of fulfilling the agency's mission to safeguard America's borders thereby protecting the public from dangerous people and materials, CBP will employ this biometric screening to confirm a traveler's identity and match the traveler to the passport they present at inspection.

However, CBP expanded the scope of the program to include all U.S. air ports of entry and first-time VWP travelers. VWP travelers already undergo biometric screening by CBP upon entry.[16]

The project has also changed from a limited time experiment to an indefinite, operational, process.

---

[8] See 8 CFR 235.1(b); and 8 U.S.C. §§1185(b) and 1185(c).
[9] See 69 FR 468, January 2004 Interim Final Rule; 69 FR 53318, August 2004 Interim Final Rule; 73 FR 77473, December 2008 Final Rule.
[14] See 8 CFR 235.1(b); and 8 U.S.C. §§1185(b) and 1185(c)
[15] See 8 CFR 235.1(b); and 8 U.S.C. §§1185(b) and 1185(c).
[16] See 69 FR 468, January 2004 Interim Final Rule; 69 FR 53318, August 2004 Interim Final Rule; 73 FR 77473, December 2008 Final Rule.

Privacy risk: None. 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).

CBP previously only retained the traveler's facial image and facial match score data during the field test, as detailed in the prior PIA. However, retention of this data included all travelers who were participants in the field test. In the expansion of this project, CBP will only retain facial images and comparison match score data from those travelers who are subject to an adverse or law enforcement action resulting from secondary inspection. All other facial images are not stored. CBP only maintains non-PII data to evaluate system performance and to report operational metrics. This data is limited to comparison match scores, number of travelers processed, and number of travelers referred to secondary. Any information CBP retains will be associated with a case file for that individual traveler and covered by the TECS SORN.[17]

Privacy risk: None. This project collects minimal PII directly from travelers who present themselves for inspection upon entry, and therefore there is no privacy risk to data minimization.

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.

During the pilot phase, the facial images were primarily used to determine the viability of using facial recognition technology to assist CBPOs in identifying possible imposters using U.S. e-passports to enter the United States. Based on the technical and operational assessment documented in the pilot's final report, the facial recognition technology proved able to enhance CBP's identification of travelers without negatively impacting port operations or traveler wait times during the pilot phase and now CBP is incorporating the technology as a routine part of entry processing.

Privacy risk: There is a risk that facial images will be used beyond the scope of an

[17] DHS/CBP-011 U.S. Customs and Border Protection TECS (December 19, 2008 73 FR 77778).

adverse action.

Mitigation: A web-based interface was created that provides specified users at the ports with the ability to find and access facial image and score data for inclusion in the case file for each individual traveler subject to an adverse action. Images are only searched using the time/date stamp, which is also included in the case file. The facial image data is not accessed or released for any unauthorized use. The program manager audits the examination, maintenance, destruction, and usage activities to ensure the data is used as described and that privacy and security protections are followed.

Privacy risk: There is a risk that facial image data may be inappropriately accessed.

Mitigation: Access to the facial image data requires a login and user account password. CBP limits real-time access to the images and limits information displayed in the system from the e-Passport to the CBPOs conducting the specific inspection. The reports can be pulled directly from the secure database by port-designated officers to be appended to the adverse action case file which provides the evidentiary information that CBP may use in prosecuting a case. Photos and score data that are retained for administrative purposes are accessible via this same database by port-designated officers.

CBPOs are not permitted to manipulate, alter, erase, reuse, modify, or tamper with any facial image data. CBP takes precautions to prevent the alteration or deletion of the facial image data to ensure that all information is accurately captured and retained. The facial image data is only stored on a CBP-approved server, which is only accessible by authorized CBP users. The facial image data is prohibited from being downloaded, manipulated, or otherwise used for personal use.

Privacy risk: There is a risk that facial image data will not be associated with the correct case file in TECS.

Mitigation: This project is not fully integrated into CBP primary and secondary processing. This represents an initial deployment of a stand-alone capability. This risk will be mitigated after a nation-wide deployment to better integrate with existing IT processing. Officers designated by the port are provided access to pull adverse action reports directly from the secure, stand-alone database.

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. Facial image data is captured in real time to obtain an accurate picture of the

individual. CBPOs are not permitted to manipulate, alter, erase, reuse, modify, or tamper with any facial image data during the pilot. Upon presentation of their travel documents, individuals interact directly with the CBPO. An individual is able to explain why his or her appearance may differ from the passport photograph, and provide additional information to assist the CBPO in determining whether the individual has properly presented his or her valid U.S. e-passport.

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.

Facial images are stored on a standalone system that does not communicate with any other CBP systems.

Privacy risk: There is a risk that CBP will create multiple standalone databases at ports of entry that have not completed IT security review and accreditation.

Mitigation: The current standalone facial comparison system is an interim step towards developing a fully integrated facial comparison capability that will share data (collected only from adverse actions) directly with existing CBP enforcement systems. When fully integrated, the authorized stand-alone database, currently storing adverse actions reports, will be decommissioned and all data will be destroyed.

This risk will be mitigated after a nation-wide deployment to better integrate with existing IT systems.

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.

All persons with access to the data are required to complete annual privacy awareness training in addition to training on ethics and the CBP Code of Conduct. CBP employees must pass a full background investigation and must also be trained regarding the access, use, maintenance, and dissemination of PII before being given access to the system maintaining the facial image data. Access controls are currently in place (including technological controls) to ensure authorized access to the facial image data.

Conclusion

As the 1:1 Facial Comparison Project continues to expand to more airports nationwide, CBP will continue to monitor the program's privacy compliance and update this PIA as necessary. This PIA will be updated as CBP's methods and policies for the use of facial recognition technology evolve.

Responsible Official

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

John Connors
Privacy Officer
Office of Privacy and Diversity
Office of the Commissioner
U.S. Customs and Border Protection

Approval Signature

Original signed copy on file with DHS Privacy Office

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security