Privacy Impact Assessment
for the U.S. Customs and Border Protection

1:1 Facial Recognition Air Entry Pilot

DHS/CBP/PIA-025

March 11, 2015

Contact Point
Patricia J. Cashin, RMP
Office of Field Operations, Entry/Exit Office
U.S. Customs and Border Protection
(202) 325-1076

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The U.S. Customs and Border Protection (CBP) is conducting the 1:1 Facial Recognition Air Entry Pilot to allow Customs and Border Protection Officers stationed at air ports of entry to use facial recognition technology as a tool to assist them in determining whether an individual presenting themselves with a valid U.S. electronic passport is the same individual photographed in that passport. The operational goals of this pilot are to determine the viability of facial recognition as a technology to assist Customs Border Protection Officers in identifying possible imposters using U.S. e-passports to enter the United States and determine if facial recognition technology can be incorporated into current CBP entry processing with acceptable impacts to processing time and the traveling public while effectively providing CBPOs with a tool to counter imposters using valid U.S. travel documents. CBP is publishing this Privacy Impact Assessment to evaluate the privacy risks of using facial recognition software at an air port of entry.

Introduction

The mission of the U.S. Customs and Border Protection (CBP) is to protect the nation from terrorists and weapons of terrorism and to foster economic security through lawful international trade and travel. CBP has identified instances when imposters have attempted to enter the United States using what appear to be valid U.S. passports. The 1:1 Facial Recognition Air Entry Pilot enables Customs Border Protection Officers (CBPO) to use facial recognition technology as a tool to assist in verifying that the person presenting the valid U.S. e-passport is also the person identified in that passport. During this pilot, CBP takes a photo of a U.S. passport holder, applies facial recognition software algorithms to compare the photo taken against the pre-existing photograph in the e-passport, and uses the results to assist in determining whether the person presenting the e-passport is the same person who was issued the e-passport.

Background

In 2007, the U.S. Department of State (DoS) 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 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 the same information visually displayed on the photo page of the passport; a biometric identifier in the form of a digital image of the passport photograph, which facilitates the use of facial recognition technology at ports-of-entry;[1]

[1] Note that although DoS has issued U.S. e-passports to U.S. citizens since August 2007, CBP has not used facial recognition technology to match the individual physically present at the port of entry with the electronic photograph from the U.S. e-passport.

the unique chip identification number; and a digital signature to protect the stored data from alteration.[2]

CBP is conducting a pilot that allows CBP Officers (CBPO) at airports to use facial recognition technology as a tool to assist them in verifying that the individual presenting a valid U.S. e-passport is the same individual identified in that passport. Two errors can occur during the entry process. The first error is known as a False Non-Match Rate (FNMR) which occurs if a CBPO fails to correctly match the e-Passport photo to the person presenting the document. A FNMR leads to increased CBPO involvement in order to verify that the individual is not an imposter. The second error is a False Acceptance Rate (FAR), which occurs when a CBPO incorrectly matches an e-passport photo with an imposter physically in front of him or her. A FAR error may allow an imposter into the United States. The facial recognition software provides the CBPO with a match confidence score after the e-passport chip is scanned and the photo is taken. The score is generated by algorithms designed to detect possible imposters. The operational goal of the 1:1 Facial Recognition Air Entry Pilot is to maximize the number of imposters caught or True Non-Match Rate (TNMR) while minimizing traveler inconvenience and CBPO impacts. Therefore, a match confidence threshold numerical score will be established to set the maximum allowable FNMR at the close of the evaluation phase of this pilot.

The operational goals of this pilot are to determine the viability of facial recognition as a technology to assist CBPOs in identifying possible imposters using U.S. e-passports to enter the United States and determine if facial recognition technology can be incorporated into current CBP entry processing with acceptable impacts to processing time and the traveling public while effectively providing CBPOs with a tool to counter imposters using valid U.S. travel documents. The overall pilot will last approximately nineteen months, including the testing and analysis phase; however, CBPOs will only the technology to capture photographs from U.S. e-passport holders for sixty days.

During this pilot, CBPOs take photographs of randomly selected U.S. e-passport holders and use facial recognition algorithms to compare the new image with the official image stored on the e-passport chip.[3] CBPOs use the facial recognition technology as another tool for determining admissibility to the United States. CBPOs will neither use the facial recognition technology output as the sole basis for whether to admit an individual into the United States nor send an individual to secondary inspection. CBP will not assign unique identification numbers to travelers based on their facial recognition algorithm. All images are only searchable by time and date stamp. At the end of the pilot, CBP will write a report with findings of the study. This report may be sent to DHS Science and Technology (S&T) and Office of Biometric Identity

[2] For more information about the U.S. e-passport, *see* http://travel.state.gov/content/passports/english/passports/FAQs.html#e-passport Frequently Asked Questions.

[3] Supervisory CBPOs (SCBPO) will set the standard for the random selection criteria and have discretion to change the criteria as needed. For example, the SCBPO may choose to select every fifth traveler but may change to every third or every seventh traveler at his or her discretion.

Management (OBIM) for awareness. DHS S&T and OBIM will not have access to the facial recognition photographs stored on the CBP server. The point of sharing the report is to provide DHS S&T and OBIM awareness of the overall findings of the pilot.

1:1 Facial Recognition Air Entry Pilot

CBP is conducting the pilot in limited air ports of entry after having successfully completed testing in a laboratory setting. The results determined that the system successfully performed matches when tested against actual passports and live captured images. The system also successfully detected imposters when presented with an imposter's passport against a live captured image.

Following the successes in a laboratory environment, CBP is now testing the facial recognition software during actual customs inspections of U.S. e-passport holders in limited air ports of entry. CBP is testing one facial match algorithm captured at the air port of entry, and then compares those results against two other algorithms in a laboratory environment. This enables CBP to conduct a comparative analysis of the performance of each algorithm. The pilot testing team uses the results to determine which algorithms were successful at maximizing the number of imposters caught while minimizing traveler inconvenience and CBPO impacts.

During the inspection process, CBPOs take a photograph of the person presenting a U.S. e-passport and compare it to the image contained in the U.S. e-passport chip using the facial recognition system. A match confidence score is generated indicating the likelihood of a match between the two photographs. For example, if an individual has a match score of ninety he or she is likely the same person in the U.S. e-passport photo. Through this pilot, CBP will determine the threshold for successful match scores and will appropriately train CBPOs that use the technology. U.S. citizens with U.S. e-passports arriving at air ports of entry testing the technology may be selected to participate in the pilot at port discretion.[4] Individuals that are selected do not have the option to opt out of this process. The facial recognition system is a tool to assist CBPOs in the inspection process. The tool does not replace officer discretion at any point within the inspection process.[5]

As part of this pilot, CBP collects the following information: photographs of travelers passing through primary inspection; facial recognition match results; issuance date of passport; CBPO determination of traveler age; and passport country of issuance (if the traveler is directed to secondary inspection).

[4] Per the previous footnote, 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.

[5] 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. A U.S. citizen must present a valid unexpired U.S. passport book upon entering the United States, unless he or she presents an excepted document. For additional information, *see* 8 CFR 253.1(b).

The purpose of the pilot is testing and evaluation of the viability of facial recognition technology; however, CBPOs are permitted to use the photographs and facial recognition match results in law enforcement proceedings if necessary. If an individual becomes the subject of an enforcement action, his or her photograph and facial recognition match result may be copied and associated per standard procedures. Any facial image data that may be used in an enforcement proceeding is governed by the system of records notice (SORN) relevant to the incident's case file. Facial image data collected by this pilot is only searchable by location or time/date stamp and is not retrieved by unique personal identifier. CBP does not share any of the facial image data that it collects using the test system with any party or organization outside of DHS. At the end of the pilot CBP may share a report of the findings of the pilot with DHS S&T and OBIM. This report will not contain personally identifiable information (PII); however, the report may contain examples of photographs. The report will describe technical and operational measures that evaluate effectiveness, suitability, and determine next steps. CBP will obscure images as needed within these reports to protect privacy of individuals participating in the pilot. All of the facial recognition photographs are hosted on a CBP server that is not accessible by any other DHS component including DHS S&T or OBIM.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 governs how the Federal Government may treat individuals and their information, and imposes obligations on federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII).[6] Section 222(2) of the Homeland Security Act directs the Chief Privacy Officer to assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act.[7]

In response to this mandate, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) that embody the 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 the Section 208 of the E-Government Act[6] and Section 222 of the Homeland Security Act of 2002.[7] CBP is conducting this FIPPs-based PIA because the 1:1 Facial Recognition Air Entry Pilot conducts privacy sensitive information collection but does not use an information technology system as defined in the E-Government Act. This PIA examines the privacy impact of 1:1 Facial Recognition Air Entry Pilot and collection of facial image data using the FIPPs.

[6] 5 U.S.C. § 552a, *as amended.*
[7] 6 U.S.C. § 142.
[6] Pub. L. 107-347; 44 U.S.C. § 3501 note.
[7] Pub. L. 107-296; 6 U.S.C. § 142.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual about its collection, use, dissemination, and maintenance of personally identifiable information (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 providing transparency to the public about this pilot by posting signage in close proximity to facial recognition camera at each testing site to inform the public that CBP is taking a photograph of U.S. e-passport holders. The signage also states that the facial images are not shared outside of DHS. The approved language is as follows: "When you present yourself for inspection to enter the United States, your photograph will be taken as part of the inspection process. The photograph will not be retained or used outside the Department of Homeland Security." This is not a Privacy Act Statement because the facial image data collected in the 1:1 Facial Recognition Air Entry Pilot is not subject to the Privacy Act because images are not retrieved by an individual's name or other unique identifier. However, this information is still considered PII since it is linkable to an individual.

CBP is also publishing this FIPPs-based PIA to provide additional public notice. CBP does not retain names, addresses, dates of birth, or other identifying characteristics during this pilot. CBP is only able to search the data by location and date/time stamp in the standalone system. Once the testing of the test system is complete CBP may determine that the technology will be used at other airports. CBP will update this PIA or issue a new PIA if the Department decides to use the technology or process beyond the pilot.

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.

Individual participation may not always be practical or possible for CBP due to CBP's law enforcement and other national security missions. CBP is authorized to collect biometric information from applicants for admission into the United States claiming to be U.S. citizens.[8] 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. 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

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

protect its borders, thereby lessening the overall security of the United States.

CBP seeks to increase individual participation in this law enforcement action by following processes and procedures already in place at ports. 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.

Images collected by the pilot that become part of a case file for a law enforcement investigation or encounter are governed by the DHS/CBP-011 TECS SORN.[9] Individuals who believe their images may have been used in a law enforcement investigation or encounter must follow the procedures outlined in the corresponding privacy documents for the TECS SORN.

3. Principle of Purpose Specification

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

The purpose of the 1:1 Facial Recognition Air Entry Pilot is to determine the viability of facial recognition technology and to assist CBPOs in identifying possible imposters using U.S. e-passports to enter the United States. CBP does not share any of the facial image data that it collects using the test system with any party outside of DHS. The only information from this pilot that may be shared is the report of the findings which may be shared with DHS S&T and OBIM.

CBP is storing the photographs in a standalone server only accessible by a small number of CBP personnel. CBP does not assign unique identification numbers to travelers based on their facial recognition algorithm. The images stored in the server are only searchable by location and time/date stamp.

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)

This is a limited duration pilot to determine the viability of facial recognition technology in order to assist CBPOs in identifying possible imposters using U.S. e-passports to enter the United States. The pilot will also help determine if facial recognition technology can be incorporated into current CBP entry processing with acceptable impacts to processing time and the traveling public while effectively providing CBPOs with a tool to counter imposters using

[9] For more information please see the DHS/CBP-011 TECS SORN, *available at*, http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm.

valid U.S. travel documents. The overall pilot will last approximately nineteen months including the testing and analysis phase. CBPOs will only take photographs for use with facial recognition software for sixty days, but will retain them for the duration of the pilot (nineteen months).

To enhance data minimization, CBP only retains the images captured using the test system for the duration of the pilot (nineteen months), unless subject to an enforcement action. The DHS/CBP-011 TECS SORN[12] provides more information about individuals who are subject to an enforcement action. The facial image data will be deleted from the CBP server at the conclusion of the pilot.

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.

CBP's primary goal is to use the images generated by the experiment for technical evaluation to determine the viability of facial recognition technology to assist CBPOs in identification of possible imposters using U.S. e-passports to enter into the United States improve business processes and national security. In some instances a photograph may become part of a case file for a law enforcement investigation or encounter. Images collected by the pilot that become part of a case file for a law enforcement investigation or encounter are governed by the DHS/CBP-011 TECS SORN and will be used for specifically for law enforcement investigations and case management. Individuals who believe their images may have been used in a law enforcement investigation or encounter must follow the procedures outlined in the corresponding privacy documents for the DHS/CBP-011 TECS SORN.

CBP does not share any of the facial image data that it collects using the test system with any party outside of DHS. The only information that is shared is the report of the findings of the pilot, which may be shared with DHS S&T and OBIM.

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.

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. CBP is taking 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 CBP. The facial image data is prohibited from being downloaded, manipulated, or otherwise used for personal

[12] For more information please see the DHS/CBP-011 TECS SORN, *available at*, http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm.

use. All facial image data is retained on a CBP-approved server and will be retained until the conclusion of the pilot. DHS S&T and OBIM may receive a report that details the findings of the study; however, neither component has access to the CBP server that stores the facial recognition images.

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.

The system is a standalone system and does not communicate with any other CBP systems. Facial image data is only stored on a CBP-approved secure server. Access to the facial data requires a login and user account password. CBP only allows CBP officials testing the system to have access to any facial image data that CBP collects. CBP also limits real-time access to the image, the results of the facial recognition algorithm, and the other information displayed in the test system from the U.S. e-passport to the CBPOs conducting the specific primary or secondary inspection. The test data is transferred via an encrypted and secure protocol and is stored in its own unique database at CBP National Data Center One (NDC1). Additionally, there is no direct application integration with any other production CBP application because this experiment is an isolated system. The facial image data is only retrievable by location and time/date stamp that signifies when and where the facial image was taken. Part of the training includes a formal evaluation that describes technical and operational measures that evaluate effectiveness, suitability, and determine next steps.

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. The facial image data is not be accessed or released for any unauthorized use. The program manager of the pilot audits the examination, maintenance, destruction, and usage activities to ensure the data is used as described and that privacy and security protections are followed.

Conclusion

CBP conducts regular self-assessments to verify compliance with its responsibilities and the privacy risk mitigations discussed in this PIA. The DHS Privacy Office also provides ongoing guidance on all privacy issues raised by significant or novel technologies. Finally, the DHS Privacy Office will be part of the process to make improvements as technology changes to make sure that all future technology is implemented consistent with all privacy policies, procedures, and applicable privacy laws. This PIA will be updated as CBP's methods and policies for the use of facial recognition technology evolve.

Responsible Officials

Patricia Cashin
Program Manager
Entry/Exit Transformation Office
Office of Field Operations
U.S. Customs and Border Protection
202-344-1076

John Connors
CBP Privacy Officer
Office of Privacy and Diversity
Office of the Commissioner
U.S. Customs and Border Protection
202-344-1610

Approval Signature

Original signed and on file at the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security