Privacy Impact Assessment
for the

Travel Document Checker Automation Using Facial Recognition

DHS/TSA/PIA-046

January 5, 2018

Contact Point
Cesar Medina
Project Manager, Innovation Task Force
Transportation Security Administration
Cesar.Medina@tsa.dhs.gov

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Transportation Security Administration (TSA) will conduct a three-week long proof of concept at Los Angeles International Airport for automating the identity verification portion of the Travel Document Checker (TDC) process using facial recognition technology. TSA will test the use of a National Institute for Standards and Technology (NIST) compliant facial matching algorithm to compare the facial images of aviation passengers who are e-Passport holders[1] on outward-bound international flights and who voluntarily enter the screening checkpoint through automated electronic security gates or "e-Gate." The e-Gate device will capture an image of the passenger's face and compare it to the biometric image in the passenger's e-Passport. The e-Gate will attempt to replicate the function of the TDC and authenticate the passenger's e-Passport and boarding pass. The operational goals of this proof of concept are to assess critical operational and technological components of the e-Gate, including the viability of using facial recognition technology for identity verification, and to capture specific metrics to inform future requirements for improving the security and speed of identity verification at airport checkpoints. TSA is publishing this Privacy Impact Assessment (PIA) to address the privacy risks inherent in the use of facial recognition technology during this proof of concept.

Introduction

Transportation Security Administration's (TSA) mission is to protect the nation's transportation systems to ensure freedom of movement for people and commerce. As part of its efforts to secure aviation transportation, TSA verifies passenger identities in order to grant access to airport sterile areas.[2] The TSA employee performing Transportation Document Checker (TDC) functions typically manually verifies identity at the checkpoint by comparing the facial photograph on a passenger's identity document to the passenger's actual face and the credential's biographic information to the biographic information on the passenger's boarding pass.[3] The TDC also checks the boarding pass and identity credential for authenticity. Once those steps are successfully completed, the passenger proceeds to security screening.

[1] E-Passports contain an electronic chip that holds the same information that is printed on the passport's data page including a digital photograph of the holder. See https://www.dhs.gov/e-passports.
[2] "Sterile areas" are portions of airports that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, or by an aircraft operator or a foreign air carrier through the screening of persons and property (49 C.F.R. § 1540.5).
[3] For passengers who are unable to present verifying identity documentation, TSA offers an alternative identity verification process in which passengers answer knowledge-based questions.

To improve the speed, efficiency, and security of existing manual identity verification,[4] TSA is exploring the use of biometrics.[5] TSA expects that facial recognition may help reduce dependencies on TSA personnel and expedite security processes - resulting in shorter lines and reduced wait times - and increase TSA's ability to detect fraudulent identity credentials. Unlike biometric matching efforts by the Department of Homeland Security (DHS) Customs and Border Protection (CBP), which involve comparing biometrics of international travelers against pre-populated galleries created from previously collected images[6], TSA seeks to verify identity by comparing the face of individuals presenting themselves to the technology against the image contained in their identification document (in this case, their passport). This approach may provide greater opportunities in future technology testing and developing requirements for biometric matching against other trustworthy identification documents such as REAL-ID compliant driver's licenses, permitting greater passenger throughput and security posture. TSA aviation authorities extend to all passengers, regardless of citizenship, and for both domestic and international flights, as well as individuals seeking to enter the sterile area of an airport.

To participate in the proof of concept, passengers (regardless of citizenship) who have a passport will choose to enter the line containing the e-Gate scanner. Signs will be posted at the line so that individuals entering the line will have notice of the proof of concept. The passenger will present their digital or paper boarding pass to the e-Gate scanner, which will capture the passenger's name. Passengers will then scan their e-Passports on the e-Gate scanner, which will check that the name on the e-Passport matches the name on the boarding pass. If the names match, the system will extract the passenger's photo from the e-Passport's embedded chip to use for facial matching. Next, the passenger will be prompted to look at the facial recognition camera, which will capture the passenger's real-time facial image. Finally, the facial recognition technology will compare the extracted e-Passport photo with the real-time facial images using a NIST-compliant facial matching algorithm. For passengers with a positive match, the e-Gate electronic security gates will open and the passengers will proceed to the TDC. For passengers who receive a negative facial match, or experience any error during the process, the e-Gate will not open and the passenger will be directed to the TDC. All passengers must complete the standard TDC process for manual identity and travel document verification, regardless of the e-Gate biometric matching results.

---

[4] *See* "Checkpoint of the Future: Evaluating TSA's Innovation Task Force Initiative," Hearing before the Transportation Subcommittee, House of Representatives, (April 27, 2017), *available at* https://homeland.house.gov/hearing/checkpoint-future-evaluating-tsas-innovation-task-force-initiative/.

[5] DHS defines biometrics as "unique physical characteristics, such as fingerprints, that can be used for automated recognition." *See* https://www.dhs.gov/biometrics. Other examples of physical characteristics that can be used for biometric authentication include DNA, face, hand, retina and iris features, and voice.

[6] *See* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-september2017.pdf and https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_26_be_mobile_air_test_06182015.pdf

TSA recognizes that its potential use of facial recognition may have significant privacy impacts for the traveling public. Accordingly, TSA will only collect personally identifiable information (PII) from e-Passport holders who volunteer to help test the technology. All facial image data will reside only momentarily on the e-Gate non-networked computer. TSA will immediately delete the PII, including the e-Passport and real-time facial images, once the passenger completes the e-Gate process. TSA will only maintain statistical data regarding the operation of the e-Gate and its components. The e-Gates will be stand-alone devices and not connected to any TSA information technology system or airport network.

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 personally identifiable information. The Homeland Security Act of 2002 Section 222(2)[7] 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 of 1974.

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.

DHS conducts PIAs on both programs and information technology systems, pursuant to Section 208[8] the E-Government Act of 2002 and Section 222[9] of the Homeland Security Act of 2002. This PIA examines the privacy impacts of the TDC Automation Proof of Concept, and its use of facial recognition technology for identification verification at airport checkpoints, as they relate 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

[7] 6 U.S.C. § 142.
[8] 44 U.S.C. § 3501 note.
[9] 6 U.S.C. § 142.

described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

TSA will provide notice at the airport on signs posted in close proximity to the e-Gate regarding the testing of facial recognition technology. In addition, TSA personnel monitoring the e-Gate technology will have hand-outs available that provide additional information about the proof of concept and where to find more information about TSA's screening technology and data protection procedures. These signs and hand-outs will also notify the public that participation in this proof of concept is completely voluntary. Finally, this PIA is published on a publicly available DHS website.

Privacy Risk: There is a risk that travelers will not know their photographs are being captured by TSA and used for identity verification.

Mitigation: This risk is mitigated. This PIA, along with hand-outs and signs posted in close proximity to the e-Gate inform the public that TSA will capture their facial image to attempt to match it with their biographic or biometric credentials located in their e-Passport to authenticate the passenger's e-Passport and boarding pass.

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.

Only travelers who volunteer to participate in the proof of concept will go through the e-Gate. Participation also is limited to individuals with e-Passports. Individuals who do not wish to participate will go through the standard TDC lane and will not be scanned by the e-Gate. Additionally, since this is only a proof of concept, all e-Passport passengers who elect to participate will still need to complete the standard TDC identity verification regardless of whether they achieve a facial match, a non-match, or an inconclusive match. TSA will also seek passengers' permission before interviewing them about their experience with the e-Gate, including passengers who decline to help test the technology. Passengers' input will be collected and stored anonymously in a password-protected file on the TSA Systems Integration Facility's Human Performance Branch shared drive. TSA will also collect statistical information regarding system performance and the number of people that decline to use the e-Gate.

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 principal purpose of using passengers' PII during this proof of concept is to assess critical operational and technological components of the e-Gate, including the viability of using facial recognition to automate the TDC process. The Aviation and Transportation Security Act (ATSA), Pub. L. 107-71, authorizes TSA to test new technology and equipment.[10] Under ATSA, TSA is responsible for, among other things, security in all modes of transportation;[11] screening operations for passenger air transportation;[12] receiving, assessing, and distributing intelligence information related at transportation security;[13] assessing threats to transportation;[14] coordinating countermeasures;[15] and carrying out such other duties relating to transportation security as it considers appropriate.[16]

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).

PII will be maintained only momentarily on the e-Gate stand-alone system during the proof of concept, and will be deleted immediately after the passenger proceeds through the e-Gate. The e-Gate is equipped with a scanner that "reads" and compares the passenger's name from the boarding pass and e-Passport. A facial scan will be generated and compared to the passenger's e-Passport photo. Once the biographic and biometric matching is completed and the passenger passes through the e-Gate, the PII, including the facial scan, will be purged from the e-Gate system. TSA will collect statistical data about the e-Gate system performance as well as anonymous passenger feedback about their experience.

Privacy Risk: There is a risk that TSA may retain passenger information longer than is necessary.

[10] 49 U.S.C § 114(f)(8), (9).
[11] 49 U.S.C. § 114(d).
[12] 49 U.S.C. § 114(e).
[13] 49 U.S.C. § 114(f)(1).
[14] 49 U.S.C. § 114(f)(2).
[15] 49 U.S.C. § 114(f)(4).
[16] 49 U.S.C. § 114(f)(15).

Mitigation: This risk is mitigated. TSA retains facial images for passengers taken by the e-Gate only as long as necessary. All facial image data only resides momentarily on the e-Gate non-networked computer, and PII is deleted from the system after the passenger passes through the e-Gate. The e-Gates are stand-alone devices and not connected to any TSA information technology system or airport network.

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.

Information garnered from the e-Gate proof of concept will be used solely for the purpose specified in the notice: to test the e-Gate's functionality and its ability to compare accurately biographic information on travel and identity documents as well as e-Passport biometric information with a passenger's facial image captured at the e-Gate. The proof of concept also may help detect fraudulent documentation. During the proof of concept, the e-Gates will not be networked with other systems. TSA will not maintain any PII after the individual passenger has completed their encounter at the e-Gate and therefore will not have any PII to share internal to or outside DHS.

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.

The purpose of the proof of concept is to assess the quality and integrity of the data that will be captured and generated at the e-Gate, and how accurately it compares the passengers' boarding pass, e-Passport, and facial image data. E-Gate passenger facial image data will be captured in real time to compare with e-Passport biometric data to test the quality and integrity of the e-Gate technology. TSA employees are not permitted to manipulate, alter, erase, reuse, modify, or tamper with any facial image during the pilot.

Privacy Risk: There is a risk that TSA's cameras will be unable to capture images of a high enough quality to produce accurate matches, resulting in TSA's inability to confirm traveler identities.

Mitigation: This risk is mitigated. Passengers who receive a negative facial match, or experience any error during the process, will be directed to the TDC. All passengers must complete

the standard TDC process for manual identity and travel document verification, regardless of the e-Gate biometric matching results.

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 e-Gate is a stand-alone system and will not communicate or connect with any TSA system or airport network. This system includes a monitoring station, consisting of a nearby lap-top manned by a TDC or TSA representative. Although the station will display the biographic and biometric matching results, the PII elements are purged immediately after matching. The TDC and e-Gate technicians will be the only personnel with access to the e-Gate monitoring station.

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 TSA and contractor personnel are required to comply with DHS/TSA privacy policies. Access controls are currently in place (including technological controls) to ensure only authorized personnel have access to the e-Gate system. The program manager of the pilot audits the examination, maintenance, destruction, and usage activities to ensure the data are used as described and that privacy and security protections are followed.

Conclusion

The identity document automation proof of concept is one of TSA's initial steps toward modernizing the airport checkpoint. The proof of concept will test the comparison of real-time facial images to e-Passport biometric images for air passengers who volunteer to go through automated e-Gates. The operational goals of this proof of concept are to assess critical operational and technological components of the e-Gate, including the viability of using facial recognition technology for identity verification, and to capture specific metrics to inform future requirements for improving the security and speed of identity verification at airport checkpoints. While the e-Gate will compare the biographic and biometric information the passenger presents to the e-Gate, no PII will be stored by the e-Gate or TSA as a result of this proof of concept. TSA envisions that

facial recognition ultimately will deliver a significant increase in passenger throughput and improvement in security at the checkpoint. This proof of concept will help determine next steps for implementing further automation of the TDC process. TSA will publish a new PIA for any further testing or deployment of a biometric-matching system.

Responsible Officials

Cesar Medina, Program Manager
Innovation Task Force
Office of Requirements and Capabilities Analysis (ORCA)
Transportation Security Administration
cesar.medina@tsa.dhs.gov

Approval Signature Page

Original, signed copy on file with the DHS Privacy Office.

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security