Privacy Impact Assessment
for the

Travel Document Checker Automation Using Facial Recognition

DHS/TSA/PIA-046(a)

August 23, 2019

Contact Point
Jason Lim
Identity Management Capability Manager
Transportation Security Administration
TSABiometrics@tsa.dhs.gov

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

Abstract

The Transportation Security Administration (TSA) will conduct a short-term proof of concept at the McCarran International Airport (LAS) for automating the identity verification portion of the Travel Document Checker (TDC) using biometric technology. TSA will assess its ability to compare the passenger's live facial image at the checkpoint against an image taken from the passenger's identity document for passengers who opt to participate. This information will be used for subsequent qualitative and quantitative analysis by the Department of Homeland Security Science and Technology (S&T) Directorate.[1] This Privacy Impact Assessment (PIA) follows TSA's previously published PIA,[2] which covered a proof of concept at the Los Angeles International Airport (LAX) for automating the identity verification portion of the TDC using facial recognition technology to capture a passenger's facial image to compare against the biometric image contained on the passenger's e-Passport. This PIA is conducted pursuant to Section 222[3] of the Homeland Security Act to address the privacy risks inherent in the use of facial recognition technology during this pilot.

Introduction

TSA's mission is to protect the nation's transportation systems to ensure freedom of movement for people and commerce. TSA aviation authorities extend to all passengers, regardless of citizenship, for both domestic and international flights, as well as individuals seeking to enter the sterile area of airports. As part of its efforts to secure aviation transportation, TSA also verifies passenger identities in order to grant access to airport sterile areas.[4] The TSA employee performing TDC functions currently verifies identity at the checkpoint by manually validating the identity document and boarding pass presented by the passenger, comparing the photograph on a passenger's identity document to the passenger's actual face, and then comparing the document's biographic information to the biographic information on the passenger's boarding pass.[5] Once those steps are successfully completed, the passenger proceeds to security screening.

To improve the speed, efficiency, and security of TSA's identity verification process, TSA is exploring the use of biometric matching technologies,[6] with a focus on facial recognition "as the

[1] In accordance with 5 U.S.C. § 552a(b)(1) and DHS/TSA-001 Transportation Security Enforcement Record System (TSERS) System of Records Routine Use A.
[2] *See* DHS/TSA/PIA-046 Traveler Document Checker Automation using Facial Recognition (January 8, 2018), *available at* https://www.dhs.gov/privacy.
[3] 6 U.S.C. § 142.
[4] "Sterile areas" are portions of airports that provide 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 CFR Part 1540.5).
[5] For passengers who are unable to present verifying identity documentation, TSA offers an alternative identity verification process in which passengers answer knowledge-based questions.
[6] DHS defines biometrics as "unique physical characteristics, such as fingerprints, that can be used for automated

primary means of identity verification for aviation security screening."[7] TSA expects that facial recognition may permit TSA personnel to focus on other critical tasks and expediting security processes – resulting in shorter lines and reduced wait times. Biometric matching is also expected to increase TSA's security effectiveness by improving the ability to detect impostors.

During the initial proof of concept at LAX discussed in the previously published PIA,[8] TSA used biometric-enabled automated electronic security gates with a camera that captured and compared a real-time facial image with the image from the passenger's e-Passport. During this next proof of concept, TSA will not use automated gates. Instead, a Credential Authentication Technology (CAT)[9] device will be equipped with a camera at the checkpoint. The CAT with Camera (CAT-C) will validate that the identity document presented by the passenger is authentic; collect the photo image and biographic information of the passenger from the document; and capture the passenger's live facial image. The CAT-C device will compare the live facial image of the individual to the image from the passenger's identity document using a proprietary facial matching algorithm to verify that the document belongs to the person presenting it. Once the facial matching result is recorded, TSA personnel staffing the CAT-C will direct the passenger to the standard TDC. All passengers must complete the standard TDC process for manual identity and travel document verification, regardless of the CAT-C biometric matching results.

The passenger's facial image, along with certain biographic information from the passenger's identity document, will be collected by TSA and retained for subsequent qualitative and quantitative analysis by S&T for this proof of concept. As discussed below in Section 4 below, the data will be obfuscated to the greatest extent possible. TSA will store this data on a removable TSA-owned encrypted hard drive attached to the CAT-C. TSA personnel will remove the encrypted hard drive daily and transfer it to S&T personnel weekly. The transfer from TSA to S&T personnel will be in person locally at LAS, in the Washington, D.C. metropolitan area, or by certified mail or courier. S&T will extract biometric images provided by TSA for the purpose of generating biometric templates from biometric images. This data transformation is not-reversible and converts biometric images into templates. Original biometric images cannot be recovered from the templates. S&T will use the data and information it receives during this pilot solely for the purpose stated in the Memoranda of Agreement (MOA) between the two agencies, and according

recognition." *See* https://www.dhs.gov/biometrics.

[7] *See* TSA Biometrics Roadmap For Aviation Security & the Passenger Experience (September 2018), *available at* www.tsa.gov.

[8] *See* DHS/TSA/PIA-046 Traveler Document Checker Automation using Facial Recognition (January 8, 2018), *available at* https://www.dhs.gov/privacy.

[9] During standard operations, CAT authenticates the security features on the identification document to validate legitimacy and collects the document's biographic data (e.g., name, date of birth, and gender) and transmits it over TSA's wireless computer network to TSA's Secure Flight database to confirm the passenger's ticketing and vetting status via TSA's Security Technology Integrated Program (STIP) interface. *See* DHS/TSA/PIA-024 Credential Authentication Technology/Boarding Pass Scanning System (CAT/BPSS) (January 18, 2013), and DHS/TSA/PIA-018 Secure Flight (July 12, 2017), *available at* https://www.dhs.gov/privacy.

to the Test Plan developed for the effort. S&T will not use the data provided by TSA for any other purpose, including operational uses within DHS. S&T will consult with the National Institutes for Standards and Technology (NIST) during the assessment of the facial-matching algorithm and to assure the analysis methodologies meet industry standards.

To participate, passengers will voluntarily choose to enter a lane dedicated to the proof of concept. Signs will be posted and hand-outs will be available so that individuals may make an informed decision about whether or not to participate. All participants, regardless of match result, will still be required to pass through the standard TDC identity verification process before being granted access to security screening.

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) 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 Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208[10] and the Homeland Security Act of 2002 Section 222. This PIA examines the privacy impact of the LAS proof of concept, and its use of facial recognition technology for identity verification at airport checkpoints, as they relate to the Fair Information Principles.

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.

[10] 44 U.S.C. § 3501

TSA will provide signage at the airport in close proximity to the proof of concept dedicated lanes to provide immediate notice to passengers. TSA personnel monitoring the CAT-C testing will have hand-outs available that provide additional information about TSA's screening technology and data protection procedures. These signs and hand-outs will also notify the public that participation is completely voluntary. TSA's strategic communications and public affairs will work to provide information about the proof of concept in advance to the public. In addition, this PIA provides notice by publication on a publicly available DHS website.

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

Mitigation: This risk is mitigated. This PIA, along with signs posted in close proximity to the CAT-C used in the proof of concept, and onsite TSA personnel with hand-outs, will inform members of the public that TSA will capture their facial images during this proof of concept and will attempt to match the facial image with the biometric data from their identity document.

Privacy Risk: There is a risk that passengers will not know that their photographs and biographic data are being transferred to and retained by S&T for qualitative and quantitative analysis.

Mitigation: This risk is mitigated. This PIA, along with signs posted in close proximity to the CAT-C used in the proof of concept, and onsite TSA personnel with hand-outs, will inform members of the public that their photographs and biographic data are being retained for S&T qualitative and quantitative analysis.

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 CAT-C. TSA plans to guide each passenger through the process. A TSA staff member will present the passenger's identity document to the CAT-C and help position the passenger for biometric capture. Individuals who do not wish to participate will go through the standard TDC lane and will not be processed by the CAT-C. Additionally, because this is only a proof of concept, all 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.

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' personally identifiable information (PII) during this proof of concept is to assess critical operational and technological components of the CAT-C, 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.[11] In ATSA, Congress gave TSA explicit authority to use biometric and other technologies to prevent persons who may pose a danger to air safety or security from boarding an aircraft.[12] TSA has authority to establish pilot programs to test new technology to ensure safety and security for the airport, including biometric technology that ensures only authorized access to secure areas.[13] The agency also has authority to strengthen access control points by deploying biometric or similar technologies to ensure security of passengers and aircraft.[14] Under ATSA, TSA is responsible for, among other things, security in all modes of transportation;[15] screening operations for passenger air transportation;[16] receiving, assessing, and distributing intelligence information related at transportation security;[17] assessing threats to transportation;[18] coordinating countermeasures;[19] and carrying out such other duties relating to transportation security as it considers appropriate.[20] Finally, the TSA Modernization Act requires a report that includes from TSA, as well as U.S. Customs and Border Patrol (CBP) specific assessments regarding the impacts of the use of biometric technology.[21]

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).

TSA will collect only the PII directly relevant and necessary to assess critical operational and technological components of the CAT-C, with a focus on the viability of using facial

[11] 49 U.S.C. § 114(f)(8), (9).
[12] Pub. L. 107-71, § 109(a)(7) (November 19, 2001) (codified at 49 U.S.C. § 114 note).
[13] 49 U.S.C. § 44903(c)(2)(3).
[14] 49 U.S.C. § 44903(g)(2)(G).
[15] 49 U.S.C. § 114(d).
[16] 49 U.S.C. § 114(e).
[17] 49 U.S.C. § 114(f)(1).
[18] 49 U.S.C. § 114(f)(2).
[19] 49 U.S.C. § 114(f)(4).
[20] 49 U.S.C. § 114(f)(15).
[21] TSA Modernization Act, Pub. L. 115-254, § 1919(c) (October 5, 2018).

recognition to automate the TDC process. TSA will only collect facial images and biographic information from passengers who opt in to the proof of concept.

TSA will collect the following passenger data: real-time images of the passenger's face (live photo from the checkpoint); passenger's photograph from the identity document; identification document issuance and expiration dates; date of travel; the type of identification document; the organization that issued the identification document (e.g., the state that issued the passenger's driver's license, or the U.S. Department of State in the case of passports); year of passenger's birth; and gender/Sex as listed in the identification document.

This information is necessary to test the viability of comparing identification documents with live facial images with the CAT-C. TSA will also collect operational metrics such as processing time and authentication rates. The operational data will be used to evaluate the potential operational impacts of using the CAT-C system for TDC operations.

Data collected during the proof of concept will also be transferred on a weekly basis to S&T for analysis. S&T will delete the data no later than 180 days following receipt in accordance with an approved TSA record retention schedule for security technology (N1-560-04-14, Item 2). S&T will evaluate the performance of the camera system (e.g., failure to acquire rate) and evaluate system matching performance (e.g., false match rate, false non-match rate). S&T will also analyze the variation in biometric performance based on reference image source (e.g., document type and document issue date). The results of the CAT-C evaluation will be used to help inform future TSA plans and biometrics requirements development and identify and mitigate any performance issues and operational concerns.

The passenger data that will be collected and transferred to S&T for analysis is as follows: real-time images of the passenger's face (live photo from the checkpoint); passenger's photograph from the identity document; identification document issuance and expiration dates; date of travel; the type of identification document; the organization that issued the identification document (e.g., the state that issued the passenger's driver's license, or the U.S. Department of State in the case of passports); year of passenger's birth; gender/Sex as listed in the identification document; obfuscated identification document number; obfuscated Passenger Name as listed in the document; and obfuscated date of birth as listed in the document. The CAT-C will "obfuscate" typewritten Personally Identifiable Information (PII) scanned from the face page of the identification document presented. This limited PII will be replaced with a code that cannot be used to recreate the PII, yet still allows confirmation that the credential is unique.

The purpose of collecting and sending the identification document number, passenger name, and year of birth is to help S&T determine if the same traveler is processed multiple times during the pilot. Without this data, it would not be possible to determine if the match is a false positive or the same passenger going through the system twice.

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

Mitigation: This risk is mitigated. TSA will collect and retain passenger PII, including biometrics, on TSA-approved removable encrypted hard drives. The removable drives will be removed from the CAT-C daily and transferred to S&T weekly. A new hard drive will be used each day to collect data from the pilot. Exchanging the hard drives will help to minimize any potential corrupted data and will allow S&T to start qualitative and quantitative analysis before the pilot concludes. S&T will maintain the data for no more than 180 days after receipt at which time it will be deleted in accordance with TSA's applicable record schedule. TSA will not separately retain the biometric or biographic data, except for storing for transfer to S&T. S&T will provide TSA with a certificate of destruction signed by its Program Manager within 60 days after the destruction of all data received from TSA, certifying that the data has been destroyed or irretrievably removed from S&T systems.

Privacy Risk: There is a risk that additional information will be captured when the identity document is imaged. In order to capture the facial image of the individual from the identity document, a photo of the front of the document is taken by the CAT-C. The process is intended to capture just the photograph of the individual and to crop all other aspects of the identity document off, but it is possible that in rare cases the cropping is not performed correctly such that additional portions of the identity document may be captured. It is possible that recognizable PII might fall within the cropped photo.

Mitigation: The risk is partially mitigated. Any additional PII that might accidentally appear in the photo is irrelevant to the proof of concept and will be disregarded.

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 CAT-C proof of concept will be used solely for the purpose specified in the notice: to test the CAT-C functionality and its ability to compare accurately a passenger's facial image on his or her identity documents with the passenger's live facial image captured by the CAT-C. There will be no negative impact to the individual from any result of the pilot or from opting not to participate. During the proof of concept, the CAT-C will not be networked with other systems. TSA will maintain limited biometric and biographic data after the individual passenger has completed his or her encounter at the CAT-C for transfer to S&T for analysis. S&T will use the information only for the assessment it is conducting for TSA for this

proof of concept. There will be no operational use by S&T, and no data sharing with other DHS components or outside of 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 pilot is to assess the quality and integrity of the data that will be captured and generated at the CAT-C, and how accurately it compares the passenger's facial image from his or her identity document with the passenger's real-time facial image. CAT-C passenger facial image data will be captured in real time to compare with the identity document biometric data to test the quality and integrity of the CAT-C technology. TSA will obtain the identity document directly from the passenger. Additionally, the passenger's facial image will be captured in real time at the checkpoint. 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. Additionally, all passengers must complete the standard TDC process for manual identity and travel document verification, regardless of the CAT-C 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 CAT-C will not communicate or connect with any TSA system or airport network during this pilot. Authorized users of the CAT-C will be limited to the TSA personnel staffing the pilot. Close accountability of the CAT-C and the removable drives will be maintained at all times. The CAT-C will be physically locked when not in use, and there will be access control on the CAT-C computer. In the unlikely event the CAT-C is tampered with or damaged, it is programmed to automatically delete all its data. The data generated during the proof of concept will be saved to a TSA-approved removable encrypted hard drive, which will be handled and stored in accordance with the *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information*.[22] TSA

[22] *See* DHS Handbook for Safeguarding Sensitive Personally Identifiable Information (December 2017), *available at*

personnel will remove the encrypted hard drive and replace it with a new hard drive daily. TSA personnel will remove the hard drives weekly and transfer them to S&T for analysis. Transfer to S&T personnel will either be in person at LAS or in the Washington, D.C. area, or the hard drives will be transferred by certified mail or courier directly to S&T. Data will be maintained, stored, transported, and accessed in accordance with TSA IT security guidelines. With the exception of the facial images, the passenger PII saved on the encrypted hard drives will be obfuscated to limit its exposure and help protect it from unauthorized access, use or disclosure during transit and while at rest.

S&T will safeguard the hard drive and the data it removes from the hard drive. S&T "test data is maintained within secured DHS facilities, using DHS firewalls, stand-alone computers, or secured computer networks. Access to test data is limited to persons with an authorized need-to-know, proper security clearances, and who have also completed annual privacy, information security, and physical security awareness courses. If the data is inaccurate, the data owner will make corrections and provide S&T with a corrected dataset. Individuals may correct data about themselves through the data owner's redress and correction process."[23]

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 may access the CAT-C. The Program Manager of the proof of concept 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 pilot will test the comparison of real-time facial images to identity document biometric images for passengers who volunteer to go through CAT-C. The operational goals of this proof of concept are to assess critical operational and technological components of the CAT-C, including the viability of using facial recognition technology for identity verification, and to capture specific metrics to inform future requirements for improving

https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information.

[23] *See* DHS/S&T/PIA-027 S&T Test Data (June 23, 2014), *available at* https://www.dhs.gov/privacy.

.

the security and speed of identity verification at airport checkpoints. 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 or updated PIA for any further testing or deployment of a biometric-matching system.

Responsible Officials

Jason Lim, Identity Management Capability Manager
TSA Biometrics
Transportation Security Administration
Department of Homeland Security

Approval Signature

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

_____

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