The
Privacy and Civil Liberties
Oversight Board

Use of Facial Recognition Technology by the Transportation Security Administration

Staff Report
May 9, 2025

[THIS PAGE INTENTIONALLY LEFT BLANK]

THE

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

USE OF FACIAL RECOGNITION TECHNOLOGY BY THE TRANSPORTATION SECURITY ADMINISTRATION

STAFF REPORT

MAY 9, 2025

Privacy and Civil Liberties Oversight Board

Beth A. Williams, Board Member

PCLOB acknowledges with gratitude the staff members who worked on this project, including Paige Anderson, Bonni Berge, Pamela Brooke, Cameron Brown, Hannah Burgess, Geoff Cohen, Jennifer Fitzpatrick, Clare Garvie, David Husband, John Leitner, Aaron Massey, Annan Mortensen, Tatjana Naquin, Alexa Potter, Alan Silverleib, and other current and former staff members.

STATEMENT FROM THE PCLOB STAFF

In 2019, the Privacy and Civil Liberties Oversight Board ("PCLOB," or "the Board") opened an oversight project on facial recognition and other biometric technologies in aviation security. PCLOB's professional staff, under the direction of PCLOB Board members, reviewed program documentation, reports, and evaluations, and worked with Department of Homeland Security offices to understand the operations of the program. This report describes the key aspects of the Transportation Security Administration's (TSA) use of facial recognition technology (FRT) to determine the identity of air travelers for security purposes. We also include an analysis of potential associated privacy and civil liberties risks and make recommendations to improve the program. The Board is currently sub-quorum, so PCLOB is issuing this report as a Staff Report, with the approval of the current Board member, per the Board's Sub-Quorum Authorities policy.

The professional staff made all final decisions with respect to this report, including selecting the topics and recommendations to include. Over the course of investigating this program and developing this report, current and former Board members and staff considered many potential topics of analysis and recommendations. Consistent with general government practice, the professional staff included only those findings and recommendations which were supported by sufficient, appropriate evidence.

As a program still in the process of development and deployment, TSA's use of FRT has not had sufficient opportunity to produce a detailed record of impact and efficacy. As such, PCLOB could not perform a thorough policy analysis for certain aspects of the program. For this reason, this report recommends that TSA make further efforts to collect information regarding the operations and performance of the program. Topics and recommendations considered, but ultimately not incorporated into this report, include issues related to program cybersecurity, additional policies and practices around signage and notice, and mechanisms for travelers to indicate affirmative opt-in consent. The absence of any particular topic or recommendation does not necessarily indicate that the staff disagree with the analysis or recommendation, but only that at this time, the staff does not assess that the available evidence provides a reasonable and sufficient basis for inclusion.

PCLOB is not the only entity examining this program, and we welcome continued conversation with Congress, other oversight bodies, TSA, civil society, and the public as the program continues to develop.

Jennifer Fitzpatrick
PCLOB Executive Director
May 9, 2025

TABLE OF CONTENTS

EXECUTIVE SUMMARY[1]

Part 1: Background, System Description, and Operation

The Transportation Security Administration (TSA) has been exploring the use of facial recognition technology (FRT) for airport security since 2017. Starting in 2023, TSA has been stationing devices with FRT capabilities at security checkpoints. These devices, known as Credential Authentication Technology-2 (CAT-2) devices, are now deployed at more than 250 U.S. airports and are used to determine the identity of travelers before those travelers are allowed to proceed through security and into the boarding areas.

TSA employs two different modes of facial recognition. In the first (called "one-to-one" or "1:1"), software compares a live photograph of the traveler to the photograph on the identity document presented by the traveler (e.g., a passport or a driver's license). In the second (called "one-to-many" or "1:N"), the traveler does not present an identity document. Instead, a Customs and Border Protection (CBP)-operated system called the Traveler Verification Service (TVS) compares the live photograph of the traveler with a gallery of pre-populated images of participating travelers expected that day at that particular airport.

One-to-One Recognition

In one-to-one mode, travelers present their identification or insert it into the device. The device reads the information from the identity document, takes a photograph of the traveler, and compares that image to the photograph on the identity document. Software determines whether the images match. If they do not, the TSA Officer at the checkpoint manually reviews the identity document and traveler and may allow the traveler to proceed. The information from the document and the live photograph are retained only for the few seconds needed to compare them, and then are deleted. Travelers may choose to opt out of this process, in which case the TSA Officer manually compares the traveler with the image on their document.

One-to-Many Recognition

The one-to-many program is currently being tested at 10 airports. To be eligible to use the one-to-many FRT system, travelers must already be enrolled in TSA PreCheck or another Trusted Traveler Program and be flying with a participating airline. Eligible travelers may choose to opt into the program when they check in. When participating travelers go through the designated checkpoint lane, the device takes a photograph and sends it to TVS, which

[1] The initiation of this oversight project was approved by a quorate Board in June 2019. The report contains the analysis of the Board's staff but has not been voted on or approved by a quorate Board.

compares it with a gallery of images of all travelers who opted into the program at that airport on that day. The results are sent back to the device and displayed to the TSA Officer. The live photograph is deleted from the device after the traveler passes through and deleted from TSA and CBP systems within 24 hours.

Part 2: Policy Analysis

Efficacy and Accuracy

TSA has asserted that evolution in techniques used by impostors and the use of fraudulent identity documents, combined with rising volumes of air travel, have strained the ability of manual identity checks to operate effectively or in a timely fashion. TSA states that by using FRT to establish that travelers match their identity documents (or images associated with their enrollment in Trusted Traveler Programs), it has more confidence that it is successfully preventing people identified as potential dangers from entering the boarding area of the airport, deterring malicious actors attempting to fly, and making the identity and boarding pass verification process more efficient.

FRT systems can experience two kinds of errors: false positives and false negatives. False positives, in which the system incorrectly asserts that two images are of the same person, may arise from impostor attempts or (for the one-to-many system) similarity with other legitimate travelers expected to fly that day. In the context of the use of FRT in TSA's security system, false positives generally would not inconvenience legitimate travelers, but could present a security issue if they allow individuals who should not be allowed access to the secure area to proceed through security. False negatives, in which the system fails to recognize an individual, primarily represent an inconvenience to the traveler. However, to the extent that such false negatives slow down processing or require additional attention from personnel, they can also impede the efficient functioning of the system.

The FRT algorithms employed by TSA are both extremely accurate according to tests performed by government laboratories. Testing by the National Institute of Standards and Technology (NIST) of the one-to-one algorithm used by TSA measured false positive rates at or below 0.001% and false negative rates below 1%, one of the best performing algorithms in NIST's dataset. For the algorithm used by TSA for one-to-many recognition, NIST testing measured false positive rates at 0.3% and false negative rates between 0.07% and 4.4%; again, one of the best performing algorithms that NIST tested.

FRT systems are known to show different failure rates for different demographic groups, a phenomenon known as "demographic differential performance." Rate disparities of false negatives mean that the burden of additional scrutiny arising from a failure of the FRT system to recognize individuals may disproportionately affect some groups, including older individuals and those that have been historically disadvantaged and marginalized.

NIST also tested the impact of demographics (including age, gender, and race) on FRT performance. For the one-to-one algorithm, the differential in false positive rates between the highest and lowest rates of any tested demographic group was approximately 0.1%; this was the lowest differential in false positives tested by NIST. The demographic group with the highest false negative rate was 0.02% more than the average across all demographic groups (0.21% as compared to 0.19%, or about 9% higher in relative terms).

In February 2024, TSA and the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) found that, for travelers processed using one-to-one facial recognition, the face capture success rate and the face matching success rate were more than 99% accurate. Neither of these rates varied based on age, gender, race, or skin tone. In the fall of 2024, using both scenario testing and operational data, TSA and DHS S&T found that, for travelers processed using one-to-many FRT, the technology was also more than 99% accurate across all demographic groups.

In an environment such as airport security, where photographs are taken in good lighting, with cooperative subjects looking directly ahead, and using high quality cameras, the accuracy of high quality FRT systems can surpass that of trained humans; that is, such FRT systems are more likely than humans to correctly identify that two images are, or are not, of the same person. FRT can also perform comparisons of faces far faster than humans. DHS found that on average, the TSA identity verification process took 22.8 seconds per person and under 30 seconds for all demographic groups.

The accuracy and speed of FRT means that the introduction of FRT is very likely to be a positive contribution to TSA's ability to determine the identity of travelers compared to the previous system of manual checks. However, because TSA does not have metrics on the number of impostors detected nor estimates of the number of impostors who are currently undetected, we are unable to evaluate the absolute contribution of the system to security or the cumulative effect of the entire passenger screening and authentication function.

Transparency and Public Notice

TSA has released multiple publicly available resources to inform the public about its use of FRT in airports and to provide details of the programs as they have been in development. TSA has also worked with Congress to provide information about TSA's use of FRT.

However, while TSA has attempted to inform the public about expansion of FRT use and general features of updated technology, there has been a lack of clear communication about the nature and maturity of plans for deployment of FRT. Terms like "pilot," "proof of concept," and "operational deployment" have been used inconsistently and can also be misleading when compared to the reality of how the technology is being used at airports. As of the publication of this report, TSA has yet to publish a single, comprehensive Privacy Impact Assessment for its use of facial recognition.

Individual Rights and Notice

According to current policy, TSA's FRT systems are voluntary, allowing for travelers to opt out of one-to-one facial matching without penalty or additional burdens, and allowing for travelers to opt in to the one-to-many system. TSA policy requires that signage be posted at all checkpoint lanes to disclose that travelers may be identified using facial recognition, that photographs will be deleted after matching, and that travelers have the right to decline participation. In early 2023, TSA stated that it had updated all CAT devices to show "clear language that notifies travelers they may decline having their photo taken." For the one-to-many system, travelers are informed of the program when they check in for their flight and are given a choice to opt in.

However, while TSA policy requires that signage and Transportation Security Officer (TSO) instruction make clear to travelers the voluntary nature of participation, there is evidence that these policies have historically not been implemented consistently. There are undeniable difficulties in establishing a program that is frequently evolving, including logistical challenges related to screening lanes and auditing performance, but travelers must be informed that they can opt out and given a meaningful opportunity to do so.

TSA and DHS also offer opportunities for travelers to submit complaints or requests for compensation for situations in which they believe that they have been harmed by actions of TSA while traveling. However, these systems do not contain options for submitting concerns or complaints specifically regarding the use of facial recognition, nor do TSA or DHS have specific procedures corresponding to such complaints. The ability to collect and respond to feedback accurately and efficiently is key for any system, and especially those that are still being developed or evaluated.

Collection, Sharing, Retention, and Use of Data

TSA's use of FRT involves multiple systems that interact with traveler information. In both the one-to-one and one-to-many systems, information is collected, transmitted, and used by TSA's Secure Flight, the TSA CAT-2 device, and DHS S&T. With one-to-many identification, information is also received from and sent to CBP's TVS. As a general matter, the more information gathered, the more places it is stored, and the longer it is retained, the higher the chance that the information could be accessed by malicious actors or misused beyond its intended purpose.

TSA has adopted a number of information security safeguards for the information it collects. Based on the available information, TSA's collection of data appears to be reasonably tailored to accomplish the operational requirements of the program. The majority of data that TSA collects is limited to the minimum amount of information needed to determine the identity of individuals at checkpoints in a reliable fashion. Live photographs taken as part of facial recognition are deleted within 24 hours and not used for any other purpose.

Safeguards Against Expansion or Misuse

Overall, given the current technical architecture and DHS policies regarding information retention and sharing, the one-to-one system presents a relatively limited risk of expansion or misuse. Clearer policies, regulatory, or statutory limitations, alongside a system of established oversight, logging, and audits, would reinforce public confidence that the system is used only for its designated purpose. Any further expansion of the scope or application of TSA's use of FRT should come only after a determination that the benefits of such expansion outweigh the increased risks to privacy and civil liberties, as well as full public disclosure and debate.

The default system configuration for one-to-one identity verification does not retain information that would be available to other entities, such as law enforcement, after the fact. The facial image and other information collected at the checkpoint only includes information required for verifying traveler identity and, in limited circumstances, assessing operational and technological components for testing and evaluation purposes. Further, the implementation of the one-to-one identity verification system does not readily lend itself to wider uses.

The one-to-many program offers more opportunities for potential expansion and for that reason has greater potential privacy and civil liberties implications. The system used for the one-to-many program retains information for a limited time and only for the purpose of determining whether a person presenting themselves at the checkpoint can be matched to a gallery of individuals who are traveling that day. However, one-to-many systems could be more easily adapted to identify individuals drawn from a larger set of people of interest.

Conclusion

Government programs that employ FRT to recognize members of the public should justify the benefit gained by employing it, operate transparently, and provide robust protection against the risks to the public's privacy and civil liberties. Use of FRT has caused concern due to its potential for use in the surveillance of public spaces, the sensitivity of the biometric data required to operate it, and documented patterns of uneven, albeit improving, demographic performance. However, as this report discusses, these risks are significantly mitigated for TSA's current FRT program.

Part 3: Recommendations

Overall Program

- **RECOMMENDATION 1:** TSA should collect and publish usage and performance data for program evaluation.

Effectiveness and Value

- **RECOMMENDATION 2:** TSA should perform operational testing of the ability of both human officers and the FRT systems to detect impostors. TSA should report the results of this testing to appropriate oversight bodies, and to the public to the extent practicable.

Demographics and Consequences of Misidentification

- **RECOMMENDATION 3:** DHS should establish standards that define minimal differential demographic performance of FRT systems and require vendors or internal developers to employ techniques that minimize such differentials.

- **RECOMMENDATION 4:** TSA should require FRT vendors to document information about the algorithm and training data employed and make that information publicly available to the extent possible consistent with national security.

Transparency

- **RECOMMENDATION 5:** TSA should regularly obtain independent assessments of staff compliance and the effectiveness of signage and training policies and practices.

- **RECOMMENDATION 6:** TSA should issue a comprehensive PIA and other privacy disclosures for the FRT programs.

- **RECOMMENDATION 7:** TSA should define and use consistent terminology to describe the deployment status of its systems.

Individual Participation

- **RECOMMENDATION 8:** TSA and DHS should establish procedures for collecting, investigating, and responding to FRT-related inquiries and complaints from travelers.

Collection, Sharing, Retention, and Use of Data

- **RECOMMENDATION 9:** TSA should not retain live photographs beyond the minimum amount of time necessary to perform matching.
- **RECOMMENDATION 10:** TSA should configure the CAT-2 devices to perform privacy-enhancing operations locally.

Safeguards Against Misuse

- **RECOMMENDATION 11:** DHS should either restore DHS Directive 026-11 to the website and affirm that it remains controlling policy, or commit to timely reissue an analogous policy.
- **RECOMMENDATION 12:** TSA, or an independent third party, should conduct regular, comprehensive audits to track compliance with privacy and civil liberties policies and procedures and evaluate their adequacy and sufficiency. TSA should make the results of such audits available to oversight bodies and, to the extent possible, to the public.
- **RECOMMENDATION 13:** DHS S&T should assess the security and privacy risks associated with the potential to reverse engineer biometric templates and identify methods to mitigate these risks. In particular, DHS S&T should investigate the applicability of privacy enhancing technologies for securely creating, processing, storing, and querying biometric templates.

Separate Statement of Board Member Beth A. Williams

Member Williams wrote to commend the Board's professional staff on producing this Report, completing a project that has been open for almost six years. She noted it accomplished an important part of the agency's mission to inform TSA's future operations and provide valuable transparency on a program that impacts privacy and civil liberties. She wrote separately to highlight four matters in her individual capacity as a Member of the Board.

First, she expressed her agreement with the staff, and endorsed their conclusion, that TSA's facial recognition program should remain voluntary for all passengers. Second, she underscored that the appropriate comparison to facial recognition technology is manual human identity matching. She endorsed the report's recommendation of operational testing of the ability of both human officers and the FRT systems to detect impostors. Third, she highlighted that in the current 1:1 system, privacy and civil liberties impacts almost entirely result from false negatives, not false positives. She urged TSA to continue to take steps to minimize differential demographic performance to the greatest extent possible, especially with regard to false negatives. Finally, she pointed out that TSA's FRT program currently has no connection to the Terrorist Watchlist, a fact that is likely unknown to many travelers. She recommended that TSA explore the national security benefit and privacy and civil liberty risks of comparing images of travelers at airport security checkpoints to images of known and suspected terrorists on the Terrorist Watchlist.

PART 1: Background, System Description, and Operation

I. Report Overview

The Transportation Security Administration (TSA) has been exploring the use of facial recognition technology (FRT) for airport security since 2017. Starting in 2023, the TSA began stationing devices with FRT capabilities at security checkpoints. These devices, which are now deployed at more than 250 U.S. airports, are used to determine the identity of travelers before they are allowed to proceed through security and into the boarding areas. This report discusses the operations of the program, provides an analysis of potential benefits and privacy risks stemming from the use of FRT, and makes a series of recommendations to improve the program.

A. History of TSA Use of Facial Recognition

TSA's mission includes securing aviation transportation, including preventing persons who may pose a danger to aviation safety or security from boarding an aircraft. Starting in 2017, TSA conducted a series of pilot tests—some in partnership with Customs and Border Protection (CBP)—to assess the feasibility of using FRT to automate traveler identity verification at airport security checkpoints.[2] In 2018, TSA signed a policy memorandum with CBP on the development and implementation of facial recognition capabilities at airports and released its strategy for deploying biometrics for aviation security, called the "Biometrics Roadmap."[3] In 2019, TSA began a series of projects (initially also described by TSA as "pilots" or "proofs of concept") to test multiple configurations of FRT using Credential Authentication Technology (CAT) devices at passenger security checkpoints in U.S. airports.

In 2020, after performing these tests, TSA acquired a new generation of CAT devices (CAT-2) with, among other features, a camera and software that can algorithmically compare an image of a traveler with the image in their presented identification document. A separate TSA technology program employed at checkpoints uses CBP's Traveler Verification System (TVS) to compare the live images of certain travelers with a pre-staged gallery of images of travelers expected at that airport on that day. Participation in these TSA systems is currently optional, either as opt-in or opt-out depending on the specific technology program.

[2] CBP began to test its own FRT system, the Traveler Verification System (TVS) in 2016 for operations at U.S. points of entry, including international airports. *See* U.S. Dep't of Homeland Sec., U.S. Customs and Border Prot., *DHS/CBP/PIA-056 Privacy Impact Assessment for the Traveler Verification Service*, at 2 (Nov. 14, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf. TVS is discussed in more detail in Part 1, Section B.1. TSA and CBP are components within the U.S. Department of Homeland Security (DHS).

[3] U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *TSA Biometrics Roadmap for Aviation Security & the Passenger Experience* (Sept. 2018). https://www.govinfo.gov/content/pkg/GOVPUB-HS4-PURL-gpo110235/pdf/GOVPUB-HS4-PURL-gpo110235.pdf [hereinafter Biometrics Roadmap].

As of April 2025, TSA had deployed more than 2,100 of these FRT-enabled CAT-2 devices at more than 250 U.S. airports.[4] TSA plans to continue to acquire and deploy additional devices. Under current procurement and funding plans, TSA expects to complete deployment of FRT-enabled devices for all checkpoints at all federalized airports[5] in the United States by 2049.[6]

B. PCLOB Project Background

The Privacy and Civil Liberties Oversight Board (PCLOB or Board) was established by the Implementing Recommendations of the 9/11 Commission Act of 2007.[7] Board Members are appointed by the President and confirmed by the Senate. PCLOB's mission is to ensure that efforts by the executive branch to protect the nation from terrorism are appropriately balanced with the need to protect privacy and civil liberties. Career professional staff assist the Board in its work.

In June 2019, the Board initiated an oversight project to review the use of biometric technologies, such as facial recognition and fingerprint scans, in aviation security. This report, prepared by the Board's professional staff, examines how TSA uses facial recognition to determine[8] a commercial air traveler's identity at security checkpoints and considers the balance of security and operational needs with privacy and civil liberties concerns.

[4] TSA Response to PCLOB Request (Apr. 17, 2025). For published numbers reflecting Fiscal Year 2024, *see also* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Credential Authentication Technology Procurement and Deployment: Fourth Quarter, Fiscal Year 2024*, at 3 (Jan. 8, 2025), https://www.dhs.gov/sites/default/files/2025-04/2025_0108_tsa_credential_authentication_technology_q4.pdf.

[5] A "federalized" airport is one for which the federal government, specifically TSA, has assumed responsibility for security under the Aviation and Transportation Security Act (ATSA) of 2001. Assumption of Civil Aviation Security Functions and Responsibilities under Chapter 449, Title 49, U.S.C., 69 Fed. Reg. 7939 (Feb. 20, 2002). There are currently more than 400 federalized airports in the United States. *See* U.S. Dep't of Homeland Sec., Transp. Sec. Admin, *TSA by the Numbers*, https://www.tsa.gov/news/press/factsheets/tsa-numbers (last visited Apr. 4, 2025).

[6] *See* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Credential Authentication Technology Procurement and Deployment: Fourth Quarter, Fiscal Year 2024*, *supra*, at 4. Because the majority of U.S. air travelers pass through a relatively small number of airports, coverage of most travelers and checkpoints would happen much sooner (and may have already happened). TSA has already deployed FRT-enabled CAT devices at a majority of federalized airports.

[7] Pub. L. 110-53, § 801, 121 Stat. 266, 352 (2007).

[8] As explained in more detail below, this report distinguishes between "identification" (discovering the identity of a previously unknown person) and "verification" (determining that a claim of identity by an individual is accurate). The catch-all phrase "determine the identity" will cover both use cases and is not meant to suggest how accurate these assessments may be.

In preparing this report, PCLOB gathered information from offices within the U.S. Department of Homeland Security (DHS) and TSA during multiple rounds of questions and responses. PCLOB reviewed disclosures, reports, and testimony, documents that describe the program and performance evaluations, and records of the acquisition program. PCLOB met with civil society groups, academic experts, and technology vendors to discuss the capabilities of FRT and to understand concerns over risks and limitations. Former Board Members and staff visited early deployments of these technologies by TSA and CBP at the Las Vegas (LAS) and Atlanta (ATL) airports in 2019 and 2020. PCLOB convened two roundtable discussions with non-governmental organizations, one with privacy and civil liberties organizations and the other with civil rights groups, to solicit viewpoints on the use and deployment of facial recognition technology in aviation security.[9]

PCLOB also considered, among other things, the U.S. National Institute of Standards and Technology's (NIST) Face Recognition Technology Evaluation (FRTE) program,[10] described in more detail below, and the 2024 National Academies of Sciences, Engineering, and Medicine report on facial recognition (NAS FR Report).[11]

C. Scope and Structure of This Report

The government uses different types of biometrics for law enforcement, identification, security, and other purposes. This report focuses on TSA's use of a specific biometric technology—facial recognition—to determine the identities of air travelers at security checkpoints. This report does not evaluate any similar CBP programs, such as CBP's use of TVS at ports of entry or exit (other than TSA's use of TVS); DHS biometric systems, such as IDENT or Homeland Advanced Recognition Technology (HART);[12] the TSA Known

[9] In PCLOB's roundtable meeting with civil society groups, organizations expressed concerns about the potential for FRT use to expand beyond the scope of aviation security, such as to law enforcement or immigration enforcement, and to create a chilling effect on Americans' civil liberties. *See, e.g.,* The Lawyers' Comm. for C.R. Under Law, *Digital Justice Initiative Comments to PCLOB Facial Recognition Roundtable* (June 30, 2020), https://lawyerscommittee.org/wp-content/uploads/2020/06/PCLOB-Facial-Recognition-Comments.pdf.

[10] NIST's program was previously known as the Face Recognition Vendor Test (FRVT). Activities within FRVT were split into FRTE, covering identification and verification, and the Face Analysis Technology Evaluation (FATE), relating to processing and analysis of images. *See* Nat'l Inst. of Standards and Tech., *Face Technology Evaluations - FRTE/FATE*, https://www.nist.gov/programs-projects/face-technology-evaluations-frtefate (last visited Apr. 4, 2025).

[11] Nat'l Acad. of Sci., Eng'g, and Med., *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, THE NAT'L ACAD. PRESS (2024), https://doi.org/10.17226/27397 [hereinafter NAS FR Report]. Note that former PCLOB Member Edward W. Felten served as co-chair of the National Academies' study committee.

[12] IDENT, also known as the Automated Biometric Identification System, is a central DHS-wide system for the storage and processing of biometric and associated information. For more information on IDENT, *see* U.S. Dep't of Homeland Sec., *DHS/OBIM/PIA-001 Automated Biometric Identification System*, https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system (last visited May 8, 2025). The Homeland Advanced Recognition Technology (HART) system is a planned replacement for

Crewmember program; CLEAR, a private third-party service which allows travelers to bypass TSA identity verification;[13] or other checkpoint developments, such as self-service and automatic gates. This report also does not address the presentation or authentication of digital identity documents (also known as mobile identification).

Part 1 of this report presents a background on facial recognition technology, an overview of TSA's role in aviation security, and a description of the current operation of the TSA facial recognition system. Part 2 contains a policy analysis of the effectiveness and value of the program, as well as the potential risks to travelers' privacy and civil liberties generated by the program and TSA's efforts to limit these risks. Part 3 contains a set of recommendations to improve the ways in which the program operates to further address potential risks to privacy and civil liberties.

IDENT. *See* U.S. Dep't of Homeland Sec., *DHS/OBIM/PIA-004(a) Privacy Impact Assessment for the Homeland Advanced Recognition Technology System (HART)* (Aug. 14, 2024), https://www.dhs.gov/sites/default/files/2024-08/24_0826_priv_pia-obim-004a-HART-update.pdf. As of 2024, it had not yet reached operational capability. *See id.* at 1.

[13] *See* CLEAR webpage, https://www.clearme.com.

II. BACKGROUND ON FACIAL RECOGNITION TECHNOLOGY

A. Biometrics and Facial Recognition

1. Definition of Biometrics

Although there is no definition of biometrics in the relevant statutes, DHS defines biometrics as "measurable biological (anatomical and physiological) or behavioral characteristics used for identification of an individual."[14] Biometric identifiers are digital representations of a physical aspect of an individual's body, such as a fingerprint, iris, or face. In most cases, a high-quality facial image belonging to an individual can uniquely identify that person.[15]

Non-biometric information about individuals (i.e., traditional records and personally identifiable information, such as name, birth date, nationality, or address) are referred to as *biographic information* or *biographics.*

2. Face Analysis and Recognition Technologies

FRT is an example of a class of artificial intelligence (AI)[16] applications that detects, analyzes, and/or recognizes human faces in digital images. Face *detection* allows software to locate the presence of faces in an image; once located, face *capture* algorithms can extract the portion (or portions) of the image containing only faces.[17] Face *analysis* attempts to identify or measure attributes of faces, such as age or emotion.[18] Face *recognition* is a technology that

[14] U.S. Dep't of Homeland Sec., *DHS Lexicon Terms and Definitions* (2017), https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf [hereinafter DHS Lexicon]. Other definitions in this section are drawn from the DHS Lexicon, DHS policy documents, and other sources.

[15] This is complicated by the challenge of distinguishing identical twins through FRT and the inherent uncertainty associated with measuring biometrics. For example, two fingerprints may indeed be unique, but a given sample, such as one found on a piece of evidence, may be insufficiently precise or complete to distinguish between multiple potential matches.

[16] There are many definitions of AI, including "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to—(A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action." 15 U.S.C. § 9401(3). More broadly, AI attempts to replicate various human intelligence-like abilities in software. For a more technical presentation of how FRT is AI, *see generally* NAS FR Report, supra.

[17] Definition adapted from: *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II: Hearing Before the H. Comm. on Homeland Sec.*, 116th Cong. 6 (2020) (testimony of Dr. Charles H. Romine, Director, NIST Info. Tech. Lab'y), https://www.govinfo.gov/content/pkg/CHRG-116hhrg41450/html/CHRG-116hhrg41450.htm.

[18] *Id.*

"compares an individual's facial features," often captured live by a camera as part of the FRT system, "to available images for verification or identification purposes."[19] Typically, FRT systems calculate a similarity score between the new image of the person and one or more reference images.

Facial recognition algorithms are most often developed using machine learning (ML) techniques. Broadly, such techniques rely on providing to the software very large data sets called "training sets." These contain pairs of images labeled as matches or non-matches. The software "learns" by repeatedly predicting whether the paired images match and adjusting the weights of its calculations to correct errors until it can perform at a desired level of accuracy. The contents and nature of the data set, such as the demographics of the people pictured, can affect the ways in which the algorithm functions.

3. Applications of FRT

In the context of aviation security, there are two key applications of FRT: verification and identification.

Verification is "the process of confirming an identity claim through facial recognition comparison."[20] For example, photographs of an individual traveler's face taken at an airport checkpoint could be compared against the preexisting digital image embedded in their passport to determine if they match—verifying the traveler is who they claim to be. Verification is commonly referred to as "1:1" (or "one-to-one") facial recognition.

Identification involves comparing a captured likeness against many images in a database to identify the image most likely to be of the same person, or to conclude that the observed person is not in the database. In some cases, these systems produce a list of multiple potential matches. Identification is commonly referred to as "1:N" (or "one-to-many") facial recognition.

Verification (1:1 facial recognition)
The process of confirming an identity claim through facial recognition comparison.

Identification (1:N facial recognition)
The process of comparing a captured likeness against many images in a database to identify the image most likely to be of the same person or to conclude that the observed person is not in the database.

[19] *Id.*; *see also* U.S. Dep't of Homeland Sec., *2024 Update on DHS's Use of Face Recognition & Face Capture Technologies* (2025), https://www.dhs.gov/archive/news/2025/01/16/2024-update-dhss-use-face-recognition-face-capture-technologies.

[20] *See supra* note 17.

B. How FRT Systems Work

FRT systems compare images of human faces to determine whether they are of the same person. Such systems are composed of multiple different technological components and processes, such as cameras, databases, computing hardware, operating software, and encoding and comparison algorithms. The accuracy and reliability of such systems depend not only on the attributes of each component, but also on how those components work together and the characteristics of the operating environment.

In most contexts, an FRT system compares a new or unknown image with one or more potential reference images. In more technical terms, for both new and reference images, a software algorithm first identifies and extracts a face likeness from a digital photograph and converts that image into a mathematical representation called a *template*. Different FRT systems use different techniques to construct templates; templates produced by different systems cannot be compared.

To identify matches, FRT algorithms compare two templates and calculate a similarity score. Similarity score values and ranges vary by vendor and implementation. Operators of a facial recognition algorithm can specify how similar templates must be for the system to consider the two corresponding face images to represent a match.[21] This process is called setting the *threshold*. If the similarity score is below that threshold, the algorithm will report a non-match, even though the live image could be of the same person as in the reference image (a so-called *false negative*, as described in more detail below). If the similarity score is above the threshold, the algorithm will report a match between the two images; if the images are in fact of different people, it is considered a *false positive*.

In 1:1 matching, the algorithm creates a template from the live image and compares that to a template of a reference photo believed to depict the traveler, such as a passport or driver's license picture. From the comparison, the algorithm generates a similarity score that quantifies the similarity of the faces in the live image and the reference photo. If the similarity score is above the set threshold, it indicates that the image is a match.

In 1:N matching, the algorithm compares a template of the live image to a set of potential matches, called a *gallery,* such as those travelers expected to board a given flight. Galleries can range in size from a few hundred to many orders of magnitude beyond that.[22] As with 1:1

[21] In some FRT systems, such as the FBI Next Generation Identification Interstate Photo System (NGI-IPS), operators do not specify a threshold. *See* Gov't Accountability Off.*, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy, GAO-16-267*, at 14 (May 2016), https://www.gao.gov/assets/gao-16-267.pdf. In such cases, the system returns the closest matches regardless of similarity score.

[22] There is no technical limit on the size of galleries. Clearview AI, a private vendor whose business is distinct from airport security and does not work with TSA, claims to use galleries containing billions of images. *Clearview AI,* https://www.clearview.ai/clearview-2-0 (last visited Apr. 9, 2025). As discussed below, TSA's 1:N

matching, the algorithm determines similarity scores. Depending on how the application is configured, the system may return the highest rated match (i.e., the image in the gallery with the highest similarity score above the threshold); no match if the highest-rated match is below the threshold; or all images with similarity scores above the threshold (also known as a "candidate list"). The "no match" case could occur if the correct face was not in the gallery (a true negative), or if the correct face was present in the gallery but the similarity score was below the threshold (a false negative).

Galleries that contain images of those individuals expected to use the system are sometimes called *closed* galleries. Examples of such include FRT systems for security, where the gallery would include all registered users of the system. Conversely, *open* galleries contain images of many individuals who aren't necessarily expected to match. Examples of FRT that use open galleries include attempting to identify attendees of public events against a police wanted list or attempting to identify images of a criminal suspect against a large gallery of mugshots. As discussed in more detail below, the galleries employed by TSA for the 1:N system are examples of closed galleries (i.e., they only contain images of users who have opted in and are expected that day) and typically currently contain no more than a few thousand images of individuals, although as the program continues to grow this number could increase to tens of thousands. TSA states that it has no plans to test open galleries and does not foresee a use case for open galleries going forward.[23]

C. Measuring FRT Performance and Accuracy

There are many ways to assess the performance of FRT systems and multiple different available metrics. The performance of a system will depend on the ways in which it is operated: environmental conditions, such as lighting or the presence of other faces or objects in the background; training of the operators; the operation of other components, such as cameras, networking, and databases; the data and methods used in training the model; and the composition of the population subjects.[24] Evaluations may also consider computational performance metrics, such as resource consumption (e.g., disk space, memory, computational demand). While this report considers only measurements of system accuracy produced by NIST and observed by DHS components, including DHS Science & Technology Directorate (S&T), TSA, and CBP, computational performance can have an important effect on system acceptability and selection.

system employs galleries typically containing no more than a few thousand images, although in the future this number could be in the tens of thousands.

[23] TSA Communication to PCLOB (Feb. 7, 2025).

[24] *See, e.g.,* Patrick Grother et al., *Face Recognition Quality Assessment: Concept and Goals, Version 1.0*, NAT'L INST. OF STANDARDS AND TECH. (2019), https://www.nist.gov/system/files/documents/2019/04/23/frvt_quality_concept_1.0.pdf.

In standard nomenclature, biometric system testing is separated into *technology* testing, which tests the performance of the technological components in idealized or laboratory conditions; *scenario* testing, which tests the system in a constructed scenario using real people; and *operational* testing, which consists of observing the system in its intended environment.[25] There is a trade-off between the ease and availability of types of testing and their reliability; obviously, one cannot perform operational testing until the system is complete, but technology and scenario testing are unlikely to predict the performance of a deployed system accurately.

False Positive

A false positive is when the system incorrectly determines that images of two different people represent the same individual, for example if the system failed to detect an impostor.

False Negative

A false negative is when the system incorrectly determines that two images of the same person are of different individuals, for example if the system failed to recognize the image on a traveler's legitimate ID as being the same person as the traveler.

Two of the core concepts in evaluating accuracy are *false positives* and *false negatives.*[26] A false positive could stem from the system failing to detect an impostor correctly, or from incorrectly identifying one individual as another. For example, it would mean a person's live image and the picture on a false identity document that they present are incorrectly identified by the system as a match, when they are not in fact images of the same person. In the context of the use of FRT in TSA's security system, false positives generally would not inconvenience legitimate travelers, but could present a security issue if they allow individuals who should not be allowed access to the secure area to proceed through security.[27] For 1:N systems, false positive rates tend to increase with gallery size, as there are more

[25] These terms and related concepts are defined by the ISO-IEC 19795 series of standards. *See* Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *ISO/IEC 19795-1:2021(en)* (2021), https://www.iso.org/standard/73515.html.

[26] The technical literature refers to the rate of false positives experienced by 1:1 systems as the "False Match Rate" (FMR) and by 1:N systems as the "False Positive Identification Rate" (FPIR); the false negative rate is the "False Non-Match Rate" (FNMR) and "False Negative Identification Rate" (FNIR) respectively. The definitions of the metrics are slightly distinct, as 1:N systems may identify more than one potential template in the gallery as a match. For readability, this report only refers to false negative rates and false positive rates for either type of system.

[27] The clearest example of a pair of images that would produce a false positive is that of a set of identical twins. Generally, both FRT systems and human reviewers are unable to correctly distinguish images of twins. As such, the incidence of twins in the population represents a ceiling on the accuracy of such systems. *See* Patrick Grother et al., *Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement,* Nat'l Inst. of Standards and Tech., at 15 (Apr. 25, 2025), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.

opportunities to incorrectly match with the probe image.

A false negative can occur when, for example, a person presents a legitimate identity document, but the system incorrectly determines that the live image and the image on the document are not of the same person. False negatives primarily represent an inconvenience to the user attempting to establish their identity, such as a traveler. False negatives may also impede the efficient functioning of the system if they slow down processing or require additional attention from system operators.

There are different reasons a system may incorrectly assess a potential match (either positively or negatively). The most obvious explanation is simply that the algorithm made an incorrect determination (i.e., produced a false positive or false negative), as described in more detail below. However, other external factors may also cause errors. The camera may fail to acquire a live photograph or may acquire one of low quality due to lighting, motion, or angle (an error type TSA refers to as a "failure to acquire"). The reference image may not have been correctly obtained (e.g., when scanning an identification document) or encoded into a template. In a 1:N system, the original reference image might not have been correctly inserted into the database or it may have been inserted with incorrect information (a class of errors known generally as "enrollment errors"). Attempting to match against less-recent photos can also produce more errors than more recent ones, though algorithms that are more accurate overall tend to be more resilient to this effect.[28]

1. The Impact of Threshold on False Positive and False Negative Rates

Most often, the focus of interest on errors is on the performance of the algorithm when all other aspects of the system (e.g., enrollment, photo acquisition, network operations) are assumed to be performing correctly. The accuracy of an FRT algorithm is influenced by the training data used in its development as well as the value of the threshold chosen (in addition to individual design and implementation decisions made by developers).

Choosing a threshold is a discretionary policy decision that involves a trade-off between false negative errors and false positive errors. Lowering the threshold makes the system accept less similar images when determining what constitutes a match, which reduces false negatives but increases false positives. This creates a heightened risk that impostors may slip through the cracks, as a false positive could result from the system incorrectly matching an impostor with someone else's identity document. Conversely, increasing the threshold causes the system to determine that fewer images are similar, which reduces false positives but

[28] Patrick Grother et al., *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification, NISTIR 8238*, NAT'L INST. OF STANDARDS AND TECH., at 7 (Nov. 2018), https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf.

increases false negatives. This relationship between threshold, false positive rates, and false negative rates is often called the "detection error trade-off."[29]

In choosing where to set the threshold, operators of a facial recognition algorithm must consider operational requirements, tolerance for or cost of errors, and the detection error trade-off curve. Consider, for example, the consequences of setting the threshold higher or lower at a security checkpoint. If the threshold is too low, there will be more false positives and it will be more likely that an impostor will be allowed to proceed through security. If the threshold is too high, there will be more false negatives and normal deviations in a person's appearance, perhaps from aging, from a different hairstyle or glasses, or from environmental conditions, such as insufficient lighting or an oblique camera angle, may result in a false non-match. In the latter scenario, some travelers might have to have their identity manually verified while fellow travelers match with facial recognition. This could inconvenience the traveler, potentially causing them to miss or delay their flight.

2. General Trends in FRT Performance

NIST's FRTE program continually evaluates the ability of FRT algorithms, including those used by TSA, to perform in a variety of challenges, such as matching photos of varying quality and resolution and, in the case of 1:N testing, doing so against galleries of differing sizes and containing differing quality images.

Since the detection error trade-off can make it difficult to summarize the performance of a system or to compare the performance of two different systems—since each system embodies a range of potential false positive and false negative rates depending on the threshold—testing is most often performed by configuring the system to operate such that one particular type of error (e.g., the false positive rate) occurs at a fixed value (e.g., 0.0001%). The test will then report the results of the other type of error (e.g., the false negative rate) that occurs in that configuration. For example, NIST testing of 1:1 systems (see below) sets the threshold for each system to produce a false positive rate of 0.0001% (i.e., one out of every one million impostor attempts is falsely considered a match) and reports the resulting false negative rate.

NIST testing focuses on algorithmic performance under a range of conditions of gallery size, image quality, and other factors. However, NIST results are not necessarily reflective of an entire system's performance as configured and deployed. FRT performance can be further affected or degraded by additional factors such as network failures, database quality issues,

[29] A. Martin et al., *The DET Curve in Assessment of Detection Task Performance*, INT'L SPEECH COMMC'N ASS'N (ISCA) (Sept. 1997), https://www.isca-archive.org/eurospeech_1997/martin97b_eurospeech.pdf.

the performance of equipment, and environmental conditions.[30] NIST recommends performing operational testing of systems.

Over the past two decades, the availability and accuracy of FRT systems has increased sharply. In a 2018 study, NIST found that facial recognition algorithms had seen "massive gains in accuracy" over the previous five years.[31] In that study, NIST tested 127 commercially available algorithms against a gallery of 26.6 million photos of good quality and found that the best algorithms, including those used by TSA, identified people correctly 99.8% of the time.[32] NIST observed that "[t]he remaining errors are in large part attributable to long-run aging and injury" of the subjects.[33] However, as discussed further below and as illustrated by a 2019 NIST study, an algorithm's error rates may vary across demographics, including age, race, and sex.[34] Nonetheless, developers have continued to improve their algorithms such that, in 2023, NIST found that algorithms are "increasingly tolerant of poorly illuminated and other low-quality images, and poorly posed subjects."[35] This trend has continued: in 2024, the NAS FR Report concluded that FRT's accuracy had "improved dramatically in the past decade."[36]

[30] *See generally* Patrick Grother et al., *Face Recognition Vendor Test (FRVT) Part 2: Identification, NISTIR 8271*, NAT'L INST. OF STANDARDS AND TECH., at 3–5 (Sept. 11, 2019), https://www.nist.gov/system/files/documents/2019/09/11/nistir_8271_20190911.pdf (discussing general parameters within which to understand the results of NIST performance tests).

[31] *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification, NISTIR 8238*, *supra*, at 2 ("The accuracy gains stem from the integration, or complete replacement, of prior approaches with those based on deep convolutional neural networks. As such, face recognition has undergone an industrial revolution, with algorithms increasingly tolerant of poor-quality images. Whether the revolution continues or has moved into a more evolutionary phase, further gains can be expected as machine learning architectures further develop, larger datasets are assembled and benchmarks are further utilized.").

[32] *Id.* at 2 ("With good quality portrait photos, the most accurate algorithms will find matching entries, when present, in galleries containing 12 million individuals, with error rates below 0.2%.").

[33] *Id.*

[34] Patrick Grother et al., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280*, NAT'L INST. OF STANDARDS AND TECH. (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[35] *See* Patrick Grother et al., *Face Recognition Vendor Test Part 2: Identification, NISTIR 8271*, NAT'L INST. OF STANDARDS AND TECH., supra, at 2; *see also Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification, NISTIR 8238*, *supra*, at 2.

[36] NAS FR Report, *supra*, at 1.

III. LEGAL AND REGULATORY CONTEXT

A. TSA's Statutory Authorities

The Aviation and Transportation Security Act (ATSA), enacted in November 2001 in the wake of the September 11 terrorist attacks, authorizes TSA to secure aviation transportation, conduct screening operations for passenger air transportation, assess threats to transportation, coordinate countermeasures, and carry out such other duties relating to transportation security as it considers appropriate.[37] TSA is specifically authorized to "identify and undertake research and development activities necessary to enhance transportation security;"[38] to "inspect, maintain, and test security facilities, equipment, and systems;"[39] and to "[p]rovide for the use of voice stress analysis, biometric, or other technologies to prevent a person who might pose a danger to air safety or security from boarding the aircraft of an air carrier or foreign air carrier in air transportation or intrastate air transportation."[40] Additionally, TSA is directed to establish pilot programs to test and evaluate new and emerging technology, including biometric technology, for providing access control and other security protections for closed or secure areas[41] of the airports.[42] The TSA Administrator is also required to "establish and carry out a program to accelerate and expand the research, development, and implementation of technologies and procedures to counteract terrorist acts against civil aviation."[43] These grants of authority have not been substantially revised or updated since the ATSA was enacted in November 2001.

B. DHS Policy Governing Facial Recognition

In September 2023, DHS issued DHS Directive 026-11, "Use of Face Recognition and Face Capture Technologies," a set of rules governing the use of facial recognition and related technologies for all DHS components.[44] These rules included requirements that FRT uses

[37] 49 U.S.C. § 114(d)–(f).

[38] 49 U.S.C. § 114(f)(8).

[39] 49 U.S.C. § 114(f)(9).

[40] 49 U.S.C. § 114 note: Enhanced Security Measures (citing Pub. L. 107-296, title XIV § 1403(b) (2002)).

[41] "Secure area" refers to the sterile area and the Secure Identification Display Area. 49 U.S.C. § 44903(h)(7)(F). Sterile area is defined as "a portion of an airport . . . that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, or by an aircraft operator . . ., through the screening of persons and property." 49 C.F.R. § 1540.5.

[42] 49 U.S.C. § 44903(c)(3).

[43] 49 U.S.C. § 44912(a)(1).

[44] U.S. Dep't of Homeland Sec., *Directive Number 026-11: Use of Face Recognition and Face Capture Technologies* (Sept. 11, 2023) [hereinafter DHS Directive 026-11].

must be tested to ensure there is no unintended bias; that in most circumstances, U.S. citizens have the right to opt out of FRT for non-law enforcement uses; and that FRT cannot be used as the sole basis of any law or civil enforcement related action. It also required a review process for all new and existing uses of FRT including by the Privacy Office, the Office for Civil Rights and Civil Liberties (CRCL), and the Office of the Chief Information Officer.[45]

In February 2025, DHS removed the text of DHS Directive 026-11 from its website. In response to PCLOB inquiries, DHS did not clarify whether DHS Directive 026-11 still applies to DHS components or whether there are specific plans to issue an updated policy that would address the same issues.

C. TSA Compliance with Congressional Reporting Requirements

Congress has mandated that TSA report on a range of actions it takes to enhance transportation security.[46]

The TSA Modernization Act instructs TSA and CBP to "consult with each other on the deployment of biometric technologies" and requires that TSA and CBP report to Congress on: (1) the operational and security impact of using biometric technology to identify travelers; (2) the potential effects on privacy of the expansion of the use of biometric technology, including methods proposed or implemented to mitigate any risks to privacy identified by the TSA Administrator or the CBP Commissioner related to the active or passive collection of biometric data; (3) the methods to analyze and address any matching performance errors related to race, gender,[47] or age identified by the TSA Administrator with respect to the use of biometric technology, including the deployment of facial recognition technology; and (4) a number of assessments as to the biometric entry-exit program.[48]

DHS submitted this report to Congress in August 2019.[49] Among other things, this report included deployment assessments for biometric technologies, such as the operational

[45] *Id.* at 5–6.

[46] *See, e.g.,* 49 U.S.C. §§ 114(s)(4)(B), 44938(a); Section 109(b) of the Aviation and Transportation Security Act (Pub. L. 107-71) (49 U.S.C. § 114 note, 115 Stat. 613–614), as amended by Pub. L. 107-296; 6 U.S.C. § 1141.

[47] While current Executive Branch policy is to use the word "sex" in place of "gender," the TSA Modernization Act uses the term "gender." Exec. Order No. 14168, Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government (Jan. 20, 2025), https://www.whitehouse.gov/presidential-actions/2025/01/defending-women-from-gender-ideology-extremism-and-restoring-biological-truth-to-the-federal-government/; TSA Modernization Act, Pub. L. 115-254 § 1919 (2018).

[48] TSA Modernization Act, Pub. L. 115-254 § 1919 (2018).

[49] U.S. Dep't of Homeland Sec., *Report to Congress, Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies* (Aug. 30, 2019). This report has been removed from the DHS website; however, an archived web version of this report can be found at:

and security impact of using biometric technology to identify travelers and potential effects on privacy.[50] However, a 2021 DHS Office of Inspector General (OIG) report found that, though TSA completed most of the statutory requirements, "the documentation TSA provided was missing portions of the requirement, such as an estimate of the rate at which fraudulent traveler credentials are rejected and an assessment of the detection percentage of fraudulent identification that could be accomplished using conventional methods."[51] A bipartisan group of twelve senators, in a letter to the DHS Inspector General in November 2024, noted, in addition, that "TSA has not provided Congress with evidence that facial recognition technology is necessary to catch fraudulent documents, decrease wait times at security checkpoints, or stop terrorists from boarding airplanes."[52]

Meanwhile, in response to congressional direction,[53] TSA has provided multiple reports to Congress detailing airports at which CAT is currently deployed, airports at which CAT is not currently deployed, and a plan for the full procurement and deployment of CAT systems at all U.S. airports.[54]

Further, Congress has required in recent years that DHS not use appropriated funds for any pilot, as defined in statute, until it reports to Congress on several aspects of the program, including an assessment methodology, an implementation plan, and any planned transition of such pilot or demonstration into an enduring program or operation.[55] TSA asserted that

https://web.archive.org/web/20240131210157/https://www.tsa.gov/sites/default/files/biometricsreport.pdf.

[50] *Id*.

[51] U.S. Dep't of Homeland Sec., Off. of Inspector Gen., *TSA Has Not Implemented All Requirements of the 9/11 Act and the TSA Modernization Act*, at 6 (Sept. 22, 2021), https://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-68-Sep21.pdf.

[52] Letter from Senators to the U.S. Dep't of Homeland Sec. Inspector Gen. (Nov. 20, 2024), https://www.merkley.senate.gov/wp-content/uploads/Merkley-Letter-to-IG-FINAL.pdf.

[53] *See, e.g.,* Consolidated Appropriations Act, Division F Joint Explanatory Statements for 2022, at 44 (2022), https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-F.pdf, and 2023, at 1331 (2023), https://www.congress.gov/117/cprt/HPRT50347/CPRT-117HPRT50347.pdf.

[54] *See Credential Authentication Technology Procurement and Deployment: Fourth Quarter, Fiscal Year 2024*, *supra*, at 3; U.S. Dep't of Homeland Sec., Transp. Sec. Admin, *Credential Authentication Technology Procurement and Deployment: First and Second Quarters* (Sept. 6, 2024), https://www.dhs.gov/sites/default/files/2024-10/2024_0906_tsa_credential_authentication_technology_procurement_and_deployment_q1_and_q2.pdf; U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Credential Authentication Technology Procurement and Deployment: Fiscal Year 2023 Report to Congress* (July 6, 2023), https://www.dhs.gov/sites/default/files/2023-08/23_0706_tsa_credential_authentication_technology.pdf.

[55] Consolidated Appropriations Act, 2023, Pub. L. 117-328, § 107, 136 Stat. 4728 (2022). Section 107 defines a pilot as "a study, demonstration, experimental program, or trial that—(1) is a small-scale, short-term experiment conducted to evaluate feasibility, duration, costs, or adverse events and improve upon the design

its demonstrations of CAT-2 1:1 and 1:N functionalities do not meet this statutory definition of a pilot.[56] Thus, TSA has not issued such a report for the use of these CAT functionalities. However, TSA describes those programs as a "proof of concept" and "pilot" in the program's Privacy Impact Assessment (PIA),[57] updated on November 28, 2023, and on TSA's own website.[58]

Despite the concerns of some members, Congress has continued to fund the expansion of TSA's facial recognition programs by regularly allocating funding for CAT machines in the annual appropriations process since at least fiscal year (FY) 2021.[59]

of an effort prior to implementation of a larger scale effort, and (2) uses more than 10 full-time equivalents or obligates, or proposes to obligate, $5,000,000 or more." A pilot does not include any "testing, evaluation, or initial deployment phase executed under a procurement contract for the acquisition of information technology services or systems, or any pilot or demonstration carried out by a non-federal recipient under any financial assistance agreement funded by DHS." *Id.*

[56] TSA asserted that the program merely enhanced the existing capabilities as part of a re-baseline, that the original intent was to deploy more broadly, and that the system was acquired through a system procurement contract, all of which are inconsistent with the statutory definition of pilot. U.S. Dep't of Homeland Sec., Transp. Sec. Admin., Memorandum, *DHS Appropriations Act, 2023, H.R.2617, Section 107 (Pilot) Applicability to Identity Management Field Demonstrations*, at 2–3 (March 8, 2023) [hereinafter IDM Section 107 Memo]. The implications of TSA's use of this terminology are discussed later in this report.

[57] U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *DHS/TSA/PIA-046(d) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, at 1–3 (Nov. 17, 2022, updated Nov. 28, 2023), https://www.dhs.gov/sites/default/files/2023-11/23_1128_priv_pia_tsa_046d_tdc.pdf. A Privacy Impact Assessment (PIA) is an analysis of how personally identifiable information is collected, stored, maintained, and disseminated. The E-Government Act of 2002 requires all federal agencies to conduct a PIA when "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form." *See* Pub. L. 107-347, § 208, 116 Stat. 2921 (2002).

[58] *See, e.g.,* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Biometrics Technology, Current Tests: Building on What TSA Has Learned*, https://www.tsa.gov/biometrics-technology ("In August 2020 at Ronald Reagan Washington National Airport (DCA), TSA demonstrated CAT-2. Based on further analysis of the DCA *pilot*, TSA conducted formal field tests with volunteer passengers at DCA, Phoenix Sky Harbor International Airport (PHX), Indianapolis International Airport (IND), and Miami International Airport (MIA) to identify, evaluate, and mitigate system performance issues across diverse operational environments and passenger demographics. In 2022, TSA started conducting additional *pilots* to further evaluate CAT-2 performance." (emphasis added)) (last visited Apr. 7, 2025).

[59] *See, e.g.,* U.S. Dep't of Homeland Sec., *FY 2024 Budget in Brief*, at 100 (2024), https://www.dhs.gov/sites/default/files/2023-03/DHS%20FY%202024%20BUDGET%20IN%20BRIEF%20%28BIB%29_Remediated.pdf; U.S. Dep't of Homeland Sec., *FY 2023 Budget in Brief*, at 102 (2023), https://www.dhs.gov/sites/default/files/2022-03/22-%201835%20-%20FY%202023%20Budget%20in%20Brief%20FINAL%20with%20Cover_Remediated.pdf; U.S. Dep't of Homeland Sec., *FY 2022 Budget in Brief*, at 95 (2022), https://www.dhs.gov/sites/default/files/publications/dhs_bib_-_web_version_-_final_508.pdf; U.S. Dep't of Homeland Sec., *FY 2021 Budget in Brief*, at 36, 83 (2021), https://www.dhs.gov/sites/default/files/publications/fy_2021_dhs_bib_0.pdf.

IV. AVIATION SECURITY AND TSA USE OF FRT

A. Risk Assessment and Traveler Information

TSA is charged with securing aviation transportation, including preventing persons who may pose a danger to aviation safety or security from boarding an aircraft. This section briefly describes some aspects of the broader TSA security approach and how FRT supplements it.

TSA describes its security architecture as a "layered" approach to securing the traveling public and the nation's transportation systems. Each layer, ranging from early detection of threats (e.g., intelligence) to last lines of defense (e.g., hardened cabin doors) is intended to deter, detect, or mitigate a terrorist attack.[60]

One such layer includes identifying travelers and evaluating the potential risk they present to security and safety. This applies to all travelers, including U.S. persons and non-U.S. persons. TSA uses a "risk-based security" strategy in its screening process, in which TSA expedites screening for known and trusted travelers (e.g., TSA PreCheck[61]) at security checkpoints and focuses resources on high-risk and unknown travelers (e.g., Selectees).[62]

This risk-based security approach requires collecting, retaining, and analyzing information about travelers. When making flight reservations, individuals must provide certain biographical information (e.g., name, sex, and date of birth). This data is transmitted to TSA as part of the Secure Flight system.[63] Secure Flight matches the information individuals provide when booking their flight to, from, within, or over the United States to

[60] *See, e.g.*, U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Layers of Security*, https://www.tsa.gov/news/press/factsheets/layers-security (last visited Apr. 8, 2025); U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Insider Threat Roadmap 2020*, at 5 (2020), https://www.tsa.gov/sites/default/files/3597_layout_insider_threat_roadmap_0424.pdf.

[61] "TSA PreCheck" is a registered trademark of TSA. All references in this report to PreCheck or TSA PreCheck refer to this mark.

[62] U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Risk-Based Security,* https://www.tsa.gov/news/press/factsheets/risk-based-security (last visited Apr. 8, 2025). For more information on DHS Trusted Traveler Programs, *see* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Trusted Traveler Programs,* https://www.dhs.gov/trusted-traveler-programs (last visited Apr. 8, 2025). For more information on "Selectees," *see* U.S. Priv. and C.L. Oversight Bd., *Report on the Terrorist Watchlist*, at 15–17 (Jan. 23, 2025), https://documents.pclob.gov/prod/Documents/OversightReport/b2f9ecff-99fc-48f9-a559-b486391b0e0a/PCLOB%20Terrorist%20Watchlist%20Report%20Unclassified.pdf.

[63] For more information about Secure Flight, *see* TSA's Secure Flight Privacy Impact Assessments. U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *DHS/TSA/PIA-018 TSA Secure Flight Program,* https://www.dhs.gov/publication/dhstsapia-018-tsa-secure-flight (last visited Apr. 8, 2025).

three subsets of the Terrorist Watchlist:[64] the No Fly List, composed of individuals who are not permitted to board an aircraft; the Selectee List, composed of individuals who receive enhanced screening; and the Expanded Selectee List, composed of individuals whose records are in the Terrorist Watchlist but are not on the No Fly or Selectee lists.[65] Individuals on the Selectee or Expanded Selectee lists are issued a boarding pass and receive enhanced screening, such as a pat down or explosives trace detection, while individuals on the No Fly List are not issued a boarding pass and are prohibited from boarding an aircraft.[66]

Additionally, TSA and CBP collect traveler information from individuals who pay to enroll in DHS Trusted Traveler Programs.[67] The TSA PreCheck program collects applicants' fingerprints and photographs as part of its enrollment and threat assessment process. The collected biometrics are linked to the traveler's biographic information. TSA issues a known traveler number (KTN) to vetted applicants who are approved, which travelers then provide to an airline when booking a travel reservation.

B. The Travel Document Checker

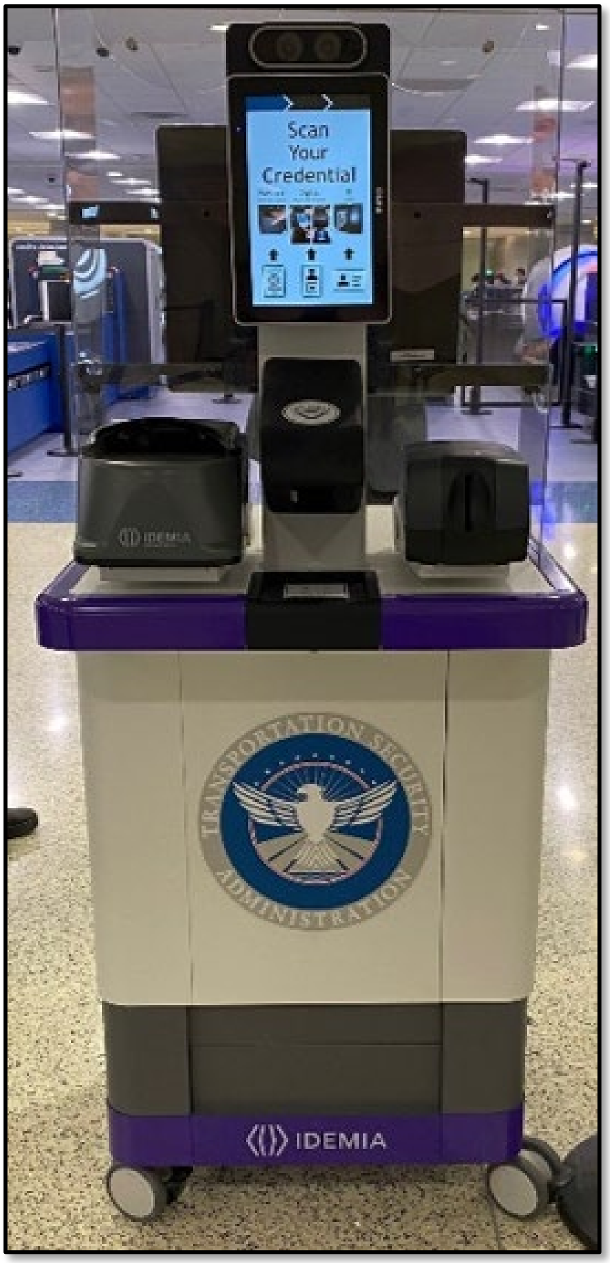
At the TSA security checkpoint, Transportation Security Officers (TSOs) perform the Travel Document Checker (TDC) function. At a TDC station, the TSO authenticates traveler identity documents, confirms that travelers match their presented identification, retrieves prescreening status information for each traveler, and confirms that travelers have valid reservations for flights that day at that terminal.

[64] The Terrorist Watchlist (or "Watchlist") is more formally referred to as the Terrorist Screening Data Set, previously called the Terrorist Screening Database. For more information, *see* U.S. Priv. and C.L. Oversight Bd., *Report on the Terrorist Watchlist* (Jan. 23, 2025), https://documents.pclob.gov/prod/Documents/OversightReport/b2f9ecff-99fc-48f9-a559-b486391b0e0a/PCLOB%20Terrorist%20Watchlist%20Report%20Unclassified.pdf.

[65] U.S. Gov't Accountability Off., *Aviation Security: TSA Coordinates with Stakeholders on Changes to Screening Rules but Could Clarify Its Review Processes and Better Measure Effectiveness, GAO-20-72*, at 5 (Nov. 2019), https://www.gao.gov/assets/gao-20-72.pdf.

[66] *Id*. at 6. Note that passengers may also receive enhanced screening based on random selection or identification by other TSA programs. *See* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Security Screening: Pat-Down Screening*, https://www.tsa.gov/travel/security-screening (last visited Apr. 8, 2025).

[67] Trusted Traveler Programs such as TSA PreCheck and Global Entry are established by Section 109(a)(3) of the ATSA, which authorizes TSA to "[e]stablish requirements to implement trusted passenger programs and use available technologies to expedite security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening." Pub. L. 107-71, 115 Stat. 597, 613 (Nov. 19, 2001). To enroll in TSA PreCheck, travelers pay a recurring enrollment fee and provide biometrics including fingerprints and photographs. DHS and FBI then perform a background check and security threat assessment. *See* U.S. Dep't of Homeland Sec., *Trusted Traveler Programs*, https://www.dhs.gov/trusted-traveler-programs (last visited Apr. 8, 2025); U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *TSA PreCheck*, https://www.tsa.gov/precheck (last visited Apr. 8, 2025).



Left: CAT-2 machine used for 1:1 FRT at a TSA security checkpoint. Image provided by TSA.

TSOs use CAT devices to perform identity document authentication and related functions (e.g., confirming that driver's licenses are non-fraudulent).[68] Prior to the use of facial recognition in the pilots described below, TSOs would manually compare the image on the identity document to the traveler's face to determine that they matched. This process is still followed at airports without facial recognition technology and for travelers who opt out. TSA acquired the first generation of CAT devices from IDEMIA[69] and began deployment in FY 2019.[70] Acquisition of the first generation of CAT devices is complete, with 2,054 CAT systems deployed at 226 airports as of May 2023.[71] Below, we describe a second generation of CAT devices configured to use FRT.

C. TSA Biometrics Strategy

TSA released the "Biometrics Roadmap" in 2018. The Biometrics Roadmap described TSA's intent to leverage biometric systems to "increase security effectiveness while also improving operational efficiency and the

[68] *See* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *DHS/TSA/PIA-046(b) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Verification*, at 1 (June 3, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa046b-tdc-june2020.pdf.

[69] Called "MorphoTrust USA" at the time of the original award in 2014. *See* Stew Magnuson, *TSA System May Make Boarding Passes Obsolete,* NAT'L DEF. (Oct. 1, 2014), https://www.nationaldefensemagazine.org/articles/2014/10/1/2014october-tsa-system-may-make-boarding-passes-obsolete. IDEMIA Group ("IDEMIA") is a multinational technology company based in France that collaborates with the federal government by offering credentialing and biometric solutions as well as secure capture and transmission of electronic fingerprints for employment, certification, licensing and other

passenger experience."[72] In particular, TSA determined that facial images would be the primary means of identity verification for aviation security screenings; at that time, TSA exclusively used manual recognition to verify the identities of travelers. TSA based this choice on three factors. First, facial recognition systems can be automated to enable passenger self-service, which reduces reliance on physical travel documents and manual inspection.[73] Second, TSA assessed that widely available, commercial off-the-shelf camera systems were capable of high performance and could be extended "across the entire passenger experience from reservation to boarding."[74] Finally, federal and state agencies that issue identity documents already collect facial images, whereas other biometrics like fingerprints or iris data are not widely available.[75]

According to TSA, one challenge to the widespread use of facial recognition in aviation security is the number of domestic travelers who do not already have facial images (e.g., a passport photo) on file with the U.S. government that could serve as reference images for FRT.[76] As discussed above, facial recognition systems for security inherently rely on the comparison between live images of individuals and known reference images. This factor influenced TSA's decision to advance with 1:1 pilot tests (which rely on passenger-provided identification rather than government holdings of biometric images) and to limit 1:N pilot

verification purposes. *See generally* IDEMIA Grp., *Making the World a Safer Place*, https://www.idemia.com/making-world-safer-place (last visited Apr. 8, 2025).

[70] *Credential Authentication Technology Procurement and Deployment: Fiscal Year 2023 Report to Congress*, *supra*, at 3; *see also* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Timeline*, https://www.tsa.gov/timeline (last visited Apr. 8, 2025).

[71] U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Credential Authentication Technology Procurement and Deployment*, at 3 (July 6, 2023), https://www.dhs.gov/sites/default/files/2023-08/23_0706_tsa_credential_authentication_technology.pdf; U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *2023 Year in Review* (2024), https://www.tsa.gov/news/press/releases/2024/01/12/2023-year-review-tsa-highlights-year-innovation-and-improvements. Note that some of these 2,054 CAT devices have already been upgraded to the second generation, as described below. *See also id.*

[72] Biometrics Roadmap, *supra*, at 5. Other biometrics, such as fingerprints, were the primary modality for enrollment in TSA's Trusted Traveler Programs. *See* Gov't Accountability Off., *Trusted Traveler Programs: DHS Has Enrollment Processes, but CBP Should Provide Additional Information on Reconsiderations, GAO-24-106314*, at 11, 16 (Feb. 2024), https://www.gao.gov/assets/gao-24-106314.pdf.

[73] Biometrics Roadmap, *supra,* at 5.

[74] *Id.*

[75] *Id*.

[76] *Id*. at 15.

tests to a subset of travelers with images on file with TSA or DHS (i.e., TSA PreCheck and Global Entry members).[77]

D. TSA Pilot Tests of FRT

TSA began testing FRT in 2017. Some early TSA FRT pilot tests explicitly required travelers to opt in and use dedicated lanes configured to use FRT-enabled test equipment.[78] In later tests, FRT-enabled devices were placed at standard checkpoints and travelers had the opportunity to opt out when they reached the TDC station.[79] Some tests only worked with travelers who already paid to enroll in TSA PreCheck, while others involved general public travelers.[80] These early tests generally affected a small number of checkpoints at participating airports, and extended for set periods of time, typically lasting a few weeks.

Due to their nature as tests, traveler information collected from these specific activities was retained for limited times and purposes, such as for analysis of de-identified outcome data by DHS S&T to evaluate the performance of the system. Information included in TSA PIAs focused only on this limited scope of testing and analysis, and the analysis of privacy risks and mitigations was restricted to those testing scenarios.[81]

The facial recognition aspect of these tests focused on two modes: 1:1, in which the traveler's live image was compared to an image in their presented identity document; and

[77] TSA PreCheck provides expedited security screening benefits for flights departing from U.S. airports. Global Entry provides expedited U.S. customs screening for international air travelers when entering the United States. Global Entry members also receive TSA PreCheck benefits as part of their membership. *See* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *What is the difference between Global Entry, TSA PreCheck and the other Trusted Traveler programs?*, https://www.tsa.gov/travel/frequently-asked-questions/what-difference-between-global-entry-tsa-precheckr-and-other (last visited Apr. 8, 2025).

[78] U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *DHS/TSA/PIA-046(a) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Recognition*, at 4 (Aug. 23, 2019), https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa-046-tdcautomationusingfacialrecognition-august2019.pdf; U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *DHS/TSA/PIA-046 Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Recognition*, at 5 (Jan. 5, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa-046-tdcautomationusingfacialrecognition-january2018.pdf.

[79] *DHS/TSA/PIA-046(b) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Verification*, *supra,* at 3.

[80] *DHS/TSA/PIA-046(d) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, *supra*, at 5, 9; U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *DHS/TSA/PIA-046(c) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, at 1, 3 (Jan. 28, 2021) https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa046c-tdcautomationusingfacialrecognition-january2021.pdf.

[81] *See DHS/TSA/PIA-046(a) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Recognition*, *supra.*

1:N, in which the traveler's live image was compared to a pre-populated gallery of images of travelers expected that day (see Section I). We describe the operations of these modes in more detail below.

E. CAT-2 Acquisition Program

Based on the results of pilot tests and evaluations of system performance, TSA decided to move ahead with acquiring a new generation of CAT devices.[82] CAT-2 deployment consists of two separate acquisition programs. In one, DHS has acquired upgrade kits to add cameras and FRT capability to existing CAT devices under a modification of the original contract.[83] In the second, DHS awarded a separate acquisition contract to IDEMIA for $128 million to acquire new CAT-2 devices,[84] and on March 28, 2024, the Acquisition Review Board approved full rate production and deployment of these new devices.[85] TSA currently uses these upgraded and new CAT-2 machines to perform 1:1 recognition at checkpoints.

On November 28, 2023, TSA announced in an updated PIA that it was beginning to test "alternate devices," such as tablets, to perform 1:N recognition at checkpoints for those passengers who have opted in to the use of FRT (as described in Section V.C., below) through participating airlines. According to TSA, these devices are configured to operate in the same way as CAT-2, including providing passengers with the same information regarding their right to opt out and avoid having their picture taken.[86] While these devices are being used to continue evaluating and testing 1:N recognition, TSA's future deployment plans will configure the CAT-2 devices to perform the 1:N recognition function as well.

F. IDEMIA FRT Algorithm Technical Capabilities

CAT-2 devices, like many other information technology systems in use by TSA and CBP, are systems composed of proprietary hardware and software produced by vendors; as described above, CAT-2 devices, which include the algorithm used by TSA to perform 1:1

[82] More specifically, on April 22, 2022, the DHS Acquisition Review Board modified the CAT program to add biometric capabilities. U.S. Dep't of Homeland Sec., *Acquisition Decision Memorandum* (Aug. 25, 2023).

[83] On June 28, 2023, DHS's Acquisition Review Board authorized full-rate production and deployment of the update kits. *Id*.

[84] U.S. Dep't of Homeland Sec., *Notice of Award: Transportation Security Administration IDIQ Contract for Next Generation Credential Authentication Technology (CAT2)* (Apr. 17, 2023), https://sam.gov/opp/d058da3afb4e4830ba8da3bcb631e360/view.

[85] U.S. Dep't of Homeland Sec., *Acquisition Decision Memorandum* (March 28, 2024) [hereinafter CAT-2 ADE-3 Increment 1 ADM].

[86] *See DHS/TSA/PIA-046(d) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, *supra*, at 1.

identity verification, are produced by IDEMIA. During the procurement process, DHS defined desired capabilities and set performance objectives for the second generation of CAT devices. However, IDEMIA, which produces the CAT-2 devices, does not disclose to the government the precise details of how those systems work, the set of images used to train the system, or other implementation details. In general, FRT vendors consider the details of their training set and algorithms to be valuable and proprietary trade secrets. The government, as the operator of the system, sets the match threshold.

According to TSA, the IDEMIA CAT-2 uses the MFACE Flex face matching algorithm to perform 1:1 matching.[87] IDEMIA publicly describes MFACE Flex as being "capable of recognizing multiple faces in industry-leading time without requiring individuals to stop, touch, or interact with the identification system."[88] It can detect and capture faces from "up to 10+ feet away."[89] MFACE Flex is also described as "suitable for various environments and a wide range of applications."[90] As developed by IDEMIA, MFACE Flex supports both 1:1 matching and 1:N matching.[91] It can perform simultaneous, multi-face tracking and capture.[92] It requires "limited user cooperation."[93] However, TSA only uses MFACE Flex in CAT-2 devices for 1:1 verification. TSA states that it has no plans to employ MFACE Flex's simultaneous capture, face tracking, or non-cooperative acquisition features.[94]

[87] TSA Responses to Second Round of PCLOB Questions, Q. 2 (Sept. 2023). Note that TSA considers the identification of the particular version of the algorithm to be Sensitive Security Information (SSI), which cannot be disclosed to the public.

[88] IDEMIA Grp., *IDEMIA launches MFACE Flex, enhancing crowd flow management with innovative facial biometrics* (Sept. 6, 2019), https://www.idemia.com/press-release/idemia-launches-mface-flex-enhancing-crowd-flow-management-innovative-facial-biometrics-2019-09-06 [hereinafter MFACE Press Release].

[89] IDEMIA Grp., *MFace Flex: Enhancing crowd flow management with innovative facial recognition,* at 1 (July 2020), https://www.idemia.com/wp-content/uploads/2021/02/mface-flex-idemia-brochure-202007.pdf.

[90] IDEMIA Grp., *MFACE™ : Keep on moving,* at 1 (Jan. 8, 2021), https://na.idemia.com/wp-content/uploads/2021/10/2021-01-08_MFace-OEM-brochure-for-ISNA.pdf.

[91] *Id*. at 2.

[92] *Id*.

[93] *Id*.

[94] TSA Response to PCLOB Request (Apr. 28, 2025).

V. TSA Policy and Standards for Operations of CAT-2 Devices for Determining Traveler Identity

This section describes TSA's policies for use of FRT in more detail, including interactions between the traveler and the checkpoint and TSA's use of traveler data.[95]

CAT-2 devices support multiple modes of determining traveler identity at the checkpoint. In one, 1:1 verification, a traveler's live image is compared to a physical identity document that they present. In a second, 1:N identification, the traveler is identified by comparing their image to a gallery of preselected images (see Section V.B.1. for further details of the gallery).[96]

TSA procedure is to provide signage at checkpoints that notifies travelers they can choose to participate in facial recognition or can opt out and proceed with manual identity verification without losing their place in the queue.[97] The instructions provided to the traveler (for example, on signage or on digital screens) further indicate that, should the traveler opt out, the traveler should inform the TSO that they decline being photographed

[95] Because the system has evolved over time during testing, and deployment and development are still in process, the descriptions in this section may differ slightly from historical or current pilot tests or locations still in the process of receiving upgraded equipment.

[96] In a third type not addressed in this report, a traveler can present a digital version of their identity document through a smartphone application, which may then be followed by a comparison between the traveler's live image and the image contained in the digital identity document. *See* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Digital Identity and Facial Recognition Technology*, https://www.tsa.gov/digital-id (last visited Apr. 16, 2025).

[97] *See DHS/TSA/PIA-046(d) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, *supra,* at 5; U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Facial Recognition Technology,* https://www.tsa.gov/news/press/factsheets/facial-recognition-technology (last visited Apr. 8, 2025). For more information on DHS privacy policy, *see* U.S. Dep't of Homeland Sec., *DHS Privacy Policy Guidance Memorandum 2008-01* (2008), https://www.dhs.gov/sites/default/files/2024-01/Fair%20Information%20Principles_12_2008.pdf; TSA Modernization Act, Pub. L. 115-254, § 1919; U.S. Dep't of Homeland Sec., *Privacy Technology Implementation Guide, Policy Directive 140-05* (2007), at 23, https://www.dhs.gov/sites/default/files/2024-03/07_0816_privtechimplementationguide_plcydirective_140-05.pdf ("The project developer should develop a mechanism that describes, to the individual, the details and context regarding the collection of PII. This notice should be made available to the individual at the same time and presented through the same method the PII is collected. If PII is collected through an online system, the notice should be provided on the same screen." . . . "The notice should generally explain: The authority enabling the collection of PII; The purpose for the collection of PII; Whether the collection of PII is mandatory or voluntary; The effects of not providing the PII; and Whether the field of PII would be shared with third parties and if so, the identity of those third parties.").

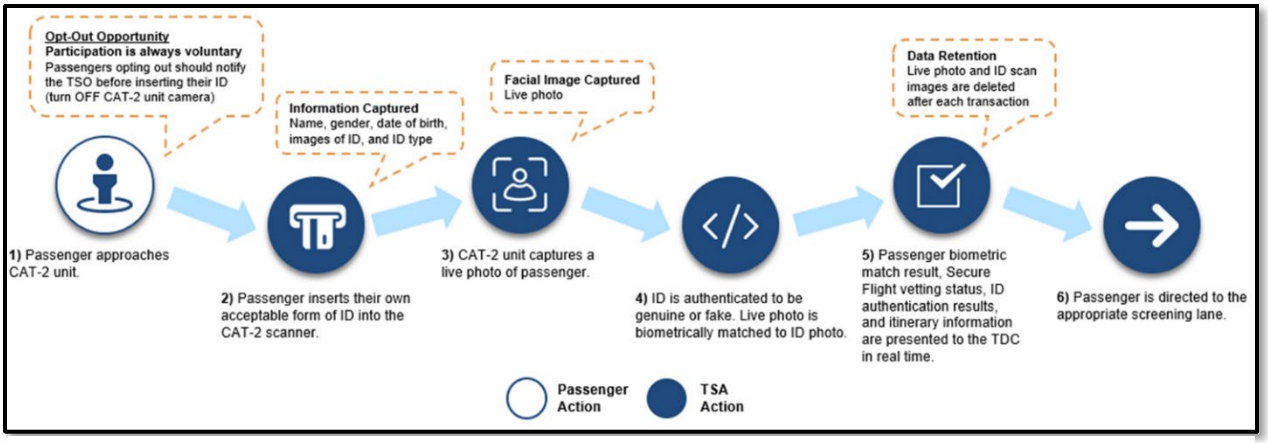
and that, if they do participate, the traveler's photo will be deleted after their identity is verified.[98]

A. 1:1 Matching

In 1:1 identity verification, a live photo of the traveler is compared to the photograph on the identity document presented by the traveler (e.g., a passport or a driver's license). For most documents, this would be a physical photograph scanned by the CAT device; for e-Passports or mobile driver's licenses, this could be a digital photograph embedded in the document or application that is transmitted to the CAT device for comparison.

TSA transmits data from Secure Flight for travelers traveling on that day at a particular airport, referred to as Secure Flight Passenger Data (SFPD), to local storage on CAT devices at that airport.[99] This transmission uses TSA secure technical infrastructure.[100] SFPD includes the self-reported biographical information provided by the traveler when they made the flight reservation, such as date of birth, name, and sex, along with flight information, such as itinerary and reservation status.[101]

Upon arrival at a checkpoint, the traveler presents their identity document to the CAT-2 by inserting it into a card reader slot or placing it on a scanner.[102] The machine scans the


Opt-Out Opportunity
Participation is always voluntary
Passengers opting out should notify the TSO before inserting their ID (turn OFF CAT-2 unit camera)
Information Captured
Name, gender, date of birth, images of ID, and ID type
Facial Image Captured
Live photo
Data Retention
Live photo and ID scan images are deleted after each transaction
1) Passenger approaches CAT-2 unit.
2) Passenger inserts their own acceptable form of ID into the CAT-2 scanner.
3) CAT-2 unit captures a live photo of passenger.
4) ID is authenticated to be genuine or fake. Live photo is biometrically matched to ID photo.
5) Passenger biometric match result, Secure Flight vetting status, ID authentication results, and itinerary information are presented to the TDC in real time.
6) Passenger is directed to the appropriate screening lane.
○ Passenger Action
● TSA Action

Above: Process flow chart for 1:1 FRT. Chart provided by TSA.

[98] *See DHS/TSA/PIA-046(d) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, *supra*, at 5.

[99] *DHS/TSA/PIA-046(b) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Verification*, *supra*, at 2.

[100] *See id.* at 2–3, 8.

[101] *Id.* at 2.

[102] *Id.* at 2–3.

document and obtains biographical information from it.[103] The CAT-2 device compares information from the document with the SFPD for that day to match the traveler with their TSA PreCheck and screening status and to confirm that the information on the document matches the information in TSA's records.[104]

Travelers that do not opt out of the use of FRT are instructed to stand in a designated location to have a photograph taken of their face.[105] The CAT-2 device uses the MFACE facial matching algorithm to compare the image from the identity document to the live image of the individual.[106] The comparison is performed on the device itself.

The CAT-2 device then displays for the TSO the live photograph of the traveler, the traveler's facial image from their identity document, the match result (that is, whether the algorithm determined that the similarity of the two images is above the set threshold), the results of the Secure Flight biographical information comparison, and any associated screening instructions.[107] If the CAT-2 device is unable to match the live image against the traveler's identification photo (whether due to the system being unable to acquire a photograph, a system failure, a match result below the threshold, or any other reason), the traveler is screened according to manual TDC processes.[108]

If a traveler opts out of having their photograph taken at the checkpoint, they are still required to provide their identity document, for example by placing it into the CAT-2 machine if the machine is able to accept that type of document.[109] The traveler is then screened according to manual TDC processes, in which the TSO manually compares the traveler's face to the photograph on their identity document. Even when not employing automated facial recognition, the TSO uses the CAT-2 device to compare the information on the identity document with passenger information supplied from Secure Flight.[110]

[103] *Id*. at 3.

[104] For example, the CAT-2 device will indicate to the TSO whether the traveler is enrolled in TSA PreCheck or not, or if they are indicated for special screening procedures. *Id*.

[105] *Id*. at 5.

[106] *Id*. at 2.

[107] *Id*. at 3.

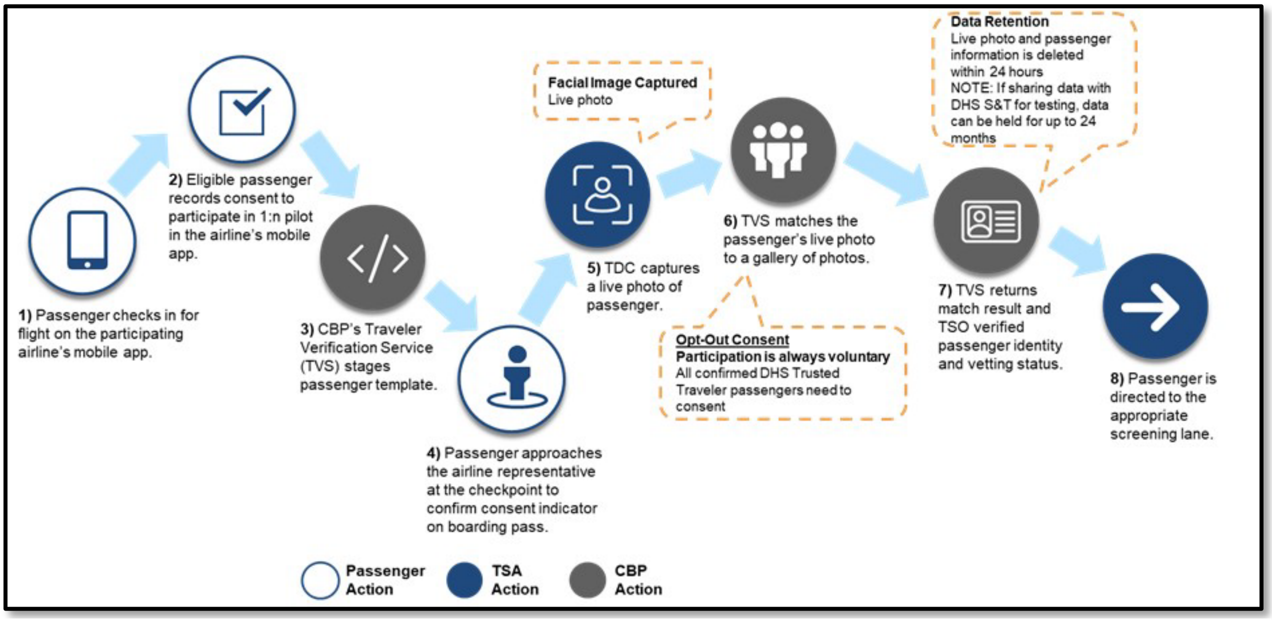
[108] *Id*. at 9.

[109] *Id*. at 3. Not all checkpoints feature CAT-2 devices configured for the traveler to insert the identification document; in other configurations, travelers hand their document to the TSO, who inserts it or scans it.

[110] *Id*.

B. 1:N Matching

TSA is also testing the use of 1:N recognition using the "TSA PreCheck Touchless ID" at 10 airports.[111] Currently, only CBP Global Entry travelers and TSA PreCheck travelers who have a U.S. passport are eligible to participate.[112] To perform the 1:N facial recognition, TSA accesses CBP's TVS to identify a traveler at the checkpoint. TVS compares the traveler's live photo to a pre-staged gallery of existing passport or traveler program enrollment photographs to identify the traveler.[113]


1) Passenger checks in for flight on the participating airline's mobile app.
2) Eligible passenger records consent to participate in 1:n pilot in the airline's mobile app.
3) CBP's Traveler Verification Service (TVS) stages passenger template.
4) Passenger approaches the airline representative at the checkpoint to confirm consent indicator on boarding pass.
Facial Image Captured
Live photo
5) TDC captures a live photo of passenger.
6) TVS matches the passenger's live photo to a gallery of photos.
Opt-Out Consent
Participation is always voluntary
All confirmed DHS Trusted Traveler passengers need to consent
Data Retention
Live photo and passenger information is deleted within 24 hours
NOTE: If sharing data with DHS S&T for testing, data can be held for up to 24 months
7) TVS returns match result and TSO verified passenger identity and vetting status.
8) Passenger is directed to the appropriate screening lane.
○ Passenger Action
● TSA Action
● CBP Action

Above: Process flow chart for 1:N FRT. Chart provided by TSA.

1. Traveler Verification Service

TVS is a cloud-based face matching service operated by CBP using equipment and algorithms developed by NEC Corporation.[114] In addition to using TVS at ports of entry to

[111] TSA Response to PCLOB Request (Apr. 17, 2025); *see* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *TSA PreCheck Touchless ID*, https://www.tsa.gov/precheck/touchless-id (last visited Apr. 18, 2025).

[112] *See* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *TSA PreCheck Touchless ID*, https://www.tsa.gov/precheck/touchless-id (last visited Apr. 18, 2025). To participate, travelers must be enrolled in a participating airline's frequent flyer program and use the airline's mobile app to opt in. *Id.*

[113] *See* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *TSA PreCheck Touchless ID*, https://www.tsa.gov/biometrics-technology/evaluating-facial-identification-technology (last visited Apr. 9, 2025).

[114] *See* U.S. Dep't of Homeland Sec., U.S. Customs and Border Prot., *DHS/CBP/PIA-056 Privacy Impact Assessment for the Traveler Verification Service*, at 6 (Nov. 14, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf; Bill Carleton, *2024 Aviation Trends: Optimizing Airport Operations with AI and Advanced Solutions*, NEC TODAY

perform biometric matching of travelers when they enter and depart the United States (e.g., at departure gates when travelers board international flights), CBP makes TVS available to TSA for use at security checkpoints, and to airlines at certain locations for functions that include baggage drop-off and check-in. TVS is a 1:N facial recognition system; that is, it compares a live image of the traveler with a gallery of images of expected travelers and returns the best match or matches, if any, above a set threshold.

The TSA 1:N system uses a gallery of photographs of participating travelers, drawn from government databases such as TSA PreCheck enrollment or U.S. passports. Using the biographic data (e.g., name, date of birth, and sex) provided by TSA PreCheck or Global Entry travelers who opted in, TSA's technical infrastructure coordinates the TVS process of querying and accessing DHS-held photographs provided when travelers registered for the Trusted Traveler Programs and U.S. passports.[115] TVS then assembles a set of images for travelers expected at each airport on that day.[116] The size of each gallery depends on the number of travelers at each airport that opt into the program; currently, galleries typically include images of a few thousand individuals, but as the 1:N program continues to grow, could contain images of tens of thousands of individuals at airports that handle more traffic. The set may include multiple images of the same traveler.[117] Each photo in the set is then converted into a biometric template and the template (not the photo itself) is temporarily stored in the TVS gallery.[118]

(June 25, 2024), https://nectoday.com/2024-aviation-trends-optimizing-airport-operations-with-ai-and-advanced-solutions/. NEC Corporation is a global commercial provider of IT services and network technologies.

[115] *See* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *TSA PreCheck Touchless ID*, https://www.tsa.gov/biometrics-technology/evaluating-facial-identification-technology (last visited Apr. 9, 2025).. More broadly, TVS can also access data that DHS already maintains, such as U.S. passport and visa photographs and photographs captured during previous airport encounters with CBP. However, TSA's use of TVS employs only Trusted Traveler Program enrollment photographs and passport photographs. *Id.*

[116] *DHS/TSA/PIA-046(d) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, *supra*, at 3.

[117] *See id.* at 9; U.S. Dep't of Homeland Sec., U.S. Customs and Border Prot., *DHS/CBP/PIA-002(e) Privacy Impact Assessment Update for the Global Enrollment System (GES): Global Entry Facial Recognition*, at 4–5 (Dec. 13, 2019), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-002e-january2020.pdf. The compilation may include multiple images of a U.S. citizen if the citizen is a Global Entry member and DHS has retained photos from the citizen's previous border crossings. Including multiple images of the same traveler in the gallery can reduce the rate of false non-matches, but can slightly increase the rate of false positive matches. *See, e.g., Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement*, *supra,* at 401–407.

[118] *DHS/CBP/PIA-056 Privacy Impact Assessment for the Traveler Verification Service*, *supra*, at 31, 39.

2. Operation

When eligible travelers check in for their flight through an airline's mobile application, they are prompted to choose whether to opt in to 1:N identification.[119] If they choose to participate, they are issued a mobile boarding pass that displays a consent indicator and TSA transmits their choice to participate from Secure Flight to CBP TVS.[120] Once at the airport, the traveler may still choose not to participate in the 1:N system. In this case, they would go through a standard checkpoint lane (e.g., TSA PreCheck) and identity verification would occur as normal.[121] However, their previously provided photo template may still be staged in the gallery.[122]

As with 1:1 identity verification, when the traveler arrives at the checkpoint, they are instructed to stand in a designated location and the CAT-2 device takes a live photograph of the traveler. In the case of 1:N identification, however, the CAT-2 device transmits the live photo to CBP TVS.[123] Within TVS, the photo is converted into a template and compared to the gallery of templates for that location.[124] Once TVS has matched the live image template with a template or templates from the gallery, TVS returns a response containing up to 10 photographs of the match (if multiple photographs of the same individual were used to populate the gallery).[125] TSA systems then correlate the match results with the traveler's data and vetting status from Secure Flight and return the data to the TDC.[126]

Because the gallery is airport-specific and includes pictures of travelers on that day, only biometric templates of facial images of passengers who have opted in through the airline and are traveling that day from that airport are staged in the CBP TVS gallery. The photographs used are encrypted while in DHS holdings, as well as during transit. The

[119] *DHS/TSA/PIA-046(d) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, *supra*, at 3.

[120] *Id.*

[121] *Id.* at 6.

[122] U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *TSA Precheck Touchless ID*, https://www.tsa.gov/biometrics-technology/evaluating-facial-identification-technology (last visited Apr. 8, 2025).

[123] *DHS/TSA/PIA-046(d) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, *supra*, at 3.

[124] *Id.*

[125] *DHS/CBP/PIA-056 Privacy Impact Assessment for the Traveler Verification Service*, *supra*, at 47.

[126] *Id.*

passenger's live photographs are deleted from the CAT-2 device and the staged images are deleted from TVS within 24 hours after the passenger's scheduled departure.

C. Current Deployment Status and Future Plans

As of April 2025, TSA had deployed more than 2,100 of FRT-enabled CAT-2 devices at more than 250 U.S. airports.[127] CAT-2 production systems, which include 1:1 recognition capability, reached operational status in March 2024.[128] By upgrading existing CAT devices and acquiring new ones, TSA plans eventually to enable 1:1 FRT at more than 400 airports.[129] TSA defines "full operational capability" (FOC) as covering all federalized checkpoint lanes, which will require 3,585 devices.[130] Under current funding levels, the program is not scheduled to reach FOC until FY 2049.[131]

As of March 2025, checkpoints at 10 airports—Atlanta (ATL), Detroit (DTW), Los Angeles (LAX), LaGuardia (LGA), John F. Kennedy (JFK), Harry Reid (LAS), Newark Liberty (EWR), O'Hare (ORD), Reagan National (DCA), and Salt Lake City (SLC)—are participating in opt-in tests of the 1:N system[132] (that is, 1:N identification), with the cooperation of three airlines (Alaska Airlines, Delta Air Lines, and United Airlines). A related program not operated by TSA, and outside the scope of this report, allows airlines to access TVS at

[127] TSA Response to PCLOB Request (Apr. 30, 2025). For published numbers reflecting Fiscal Year 2024, *see also* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Credential Authentication Technology Procurement and Deployment: Fourth Quarter, Fiscal Year 2024*, at 3 (Jan. 8, 2025), https://www.dhs.gov/sites/default/files/2025-04/2025_0108_tsa_credential_authentication_technology_q4.pdf.

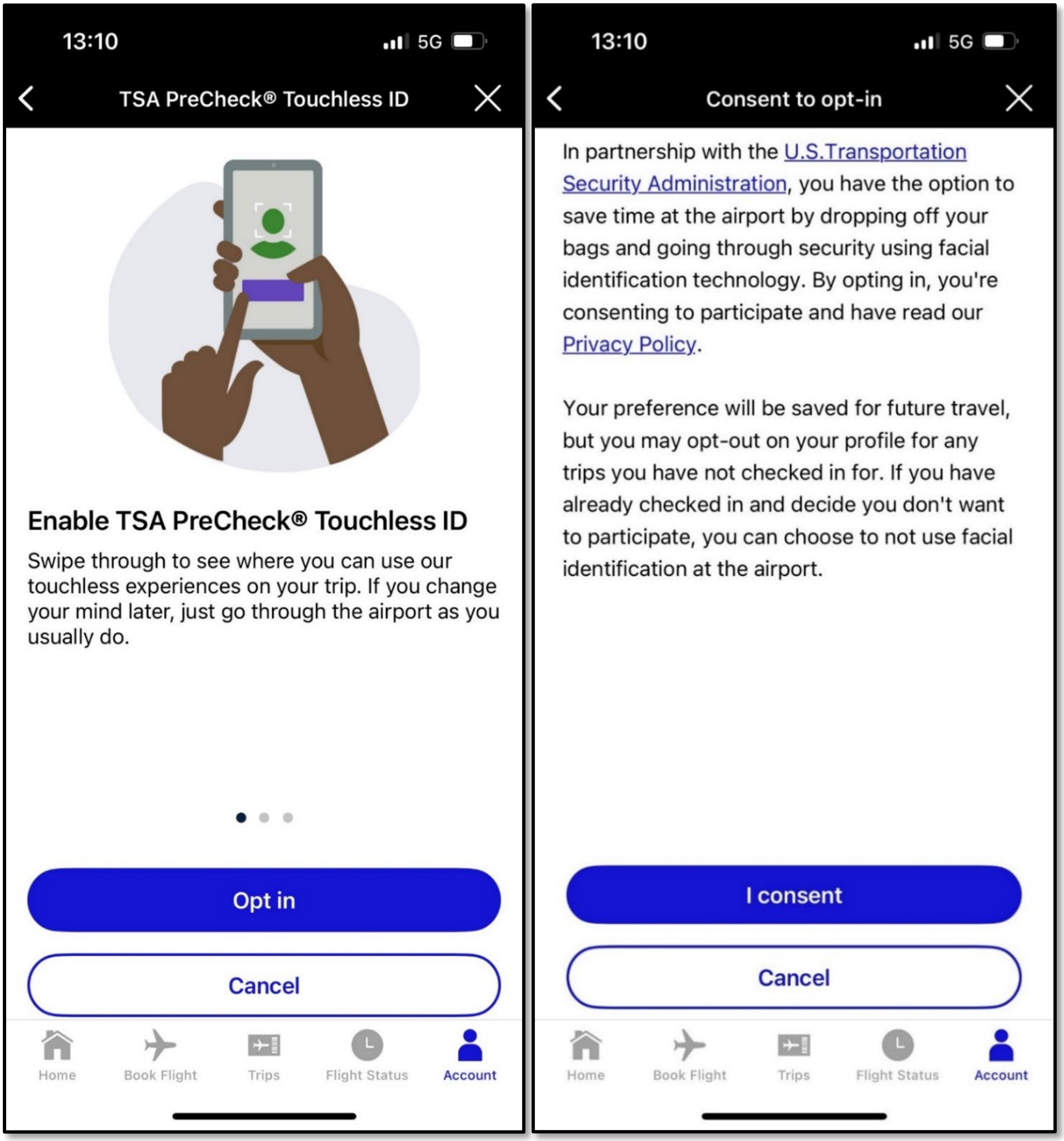
[128] TSA Responses to Fourth Round of PCLOB Questions (Feb. 2024). Formally, DHS refers to this stage of an acquisition program as an Acquisition Decision Event 3 (ADE-3). CAT-2 ADE-3 Increment 1 ADM, *supra*.

[129] U.S. Dep't of Homeland Sec., *Facial Recognition Technology*, https://www.tsa.gov/news/press/factsheets/facial-recognition-technology (last visited Apr. 9, 2025); *Credential Authentication Technology Procurement and Deployment: Fourth Quarter, Fiscal Year 2024*, *supra,* at 3.

[130] Dep't of Homeland Sec., Transp. Sec. Admin., *Credential Authentication Technology Procurement and Deployment: Third Quarter*, at ii (Nov. 27, 2024), https://www.dhs.gov/sites/default/files/2025-02/2024_1127_tsa_credential_authentication_technology_q3_0.pdf.

[131] *Credential Authentication Technology Procurement and Deployment: Fourth Quarter, Fiscal Year 2024*, *supra,* at ii; TSA Responses to Third Round of PCLOB Questions (Dec. 2023). Note that "Full Operational Capability" indicates the point in time in which every checkpoint in every airport with federal security has sufficient CAT-2 devices to serve all travelers. Coverage of the majority of travelers, checkpoints, or airports would happen much sooner.

[132] *See* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *TSA PreCheck Touchless ID*, https://www.tsa.gov/precheck/touchless-id (last visited Apr. 9, 2025). TSA refers to this more formally as "TSA PreCheck Touchless ID," while different airlines use different branding (e.g., "Delta Digital ID"). We will refer to it in this report as the "1:N system."



Enable TSA PreCheck® Touchless ID

Swipe through to see where you can use our touchless experiences on your trip. If you change your mind later, just go through the airport as you usually do.

In partnership with the U.S.Transportation Security Administration, you have the option to save time at the airport by dropping off your bags and going through security using facial identification technology. By opting in, you're consenting to participate and have read our Privacy Policy.

Your preference will be saved for future travel, but you may opt-out on your profile for any trips you have not checked in for. If you have already checked in and decide you don't want to participate, you can choose to not use facial identification at the airport.

Above: Opting in to 1:N FRT using United Airlines' mobile app. Images provided by TSA.

baggage drop and boarding locations.[133] TSA had plans to expand the number of airport locations for the 1:N program to 10 airports by the end of 2024.[134] A final decision as to whether to proceed with operational deployment of the 1:N system is expected to occur in 2025.

In a 2023 Government Accountability Office (GAO) study, TSA officials told GAO that "TSA continues to explore adding additional capabilities to the technology in future increments and expanding its uses outside of checkpoint security to the overall aviation infrastructure."[135] That year, then-TSA Administrator David Pekoske publicly stated that travelers' current "option to opt out without a time penalty" is in effect while the program is in the "operational assessment phase" and that "[e]ventually we will get to the point where we will require biometrics across the board because it is much more effective, much more efficient."[136] However, adopting such mandatory use of biometrics for non-law enforcement purposes would require changes to or repeal of DHS Directive 026-11.[137] TSA states that it currently has no plans to mandate the use of FRT at airport checkpoints for identity verification purposes.[138]

[135] U.S. Gov't Accountability Off., *DHS Annual Assessment: Major Acquisition Programs Are Generally Meeting Goals, but Cybersecurity Policy Needs Clarification, GAO-23-106701*, at 40 (Apr. 2023), https://www.gao.gov/assets/d23106701.pdf.

[136] *Accelerating Aviation Security: Innovative New Technology Keeping The Skies Safe*, at 07:45–08:31 (March 14, 2023), https://schedule.sxsw.com/2023/events/PP1143589.

[137] DHS Directive 026-11 states in part that when FRT is used for verification for non-law enforcement-related actions or investigations, U.S. citizens are generally afforded the right to opt out and should be offered alternative processing. DHS Directive 026-11, *supra,* at 6. However, as discussed above, the status of DHS 026-11 is unclear.

[138] TSA Communication to PCLOB (Feb. 7, 2025).

PART 2: Policy Analysis

I. INTRODUCTION TO POLICY ANALYSIS

PCLOB's enabling statute instructs PCLOB to "analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties," and to "ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism."[139] In this section, we discuss TSA's use of FRT and assess the value of TSA's FRT program, the extent to which privacy and civil liberties concerns are appropriately considered in the operation of the program, and whether the national security benefits of this program are properly balanced with the protection of the public's privacy and civil liberties. This report considers the value and risks of the introduction of FRT into TSA's system; we do not address issues associated with TSA's underlying security approach, e.g., the need for credential authentication, the need for reliable identification of travelers, or the operations of the Secure Flight program.

We begin with background to our analysis: public concern over FRT, the sensitivity of biometric data, and the challenges of evaluating a program that has shifted from a limited pilot to a far broader and eventual nationwide deployment. This is followed by an analysis of the value and effectiveness of the program.

We then discuss individual elements of privacy and civil liberties risks and protections related to the use of FRT: consequences of misidentification, including differential demographic patterns; public notice and transparency; rights of individual participation; the collection, sharing, retention, and use of biometric data; and safeguards against misuse of biometric data or facial recognition technology. Within each section, we describe how those protections are implicated in the program, detail how TSA currently addresses them, and assess whether the risks are appropriately considered and mitigated by current practices. Where appropriate, we provide recommendations to better address privacy and civil liberties concerns.

We conclude by assessing the overall contributions and risks of the program, and by suggesting further improvements to assess the effectiveness and value of the program and the impact on travelers, as well as to establish further protections for privacy and civil liberties.

[139] 42 U.S.C. § 2000ee(c).

A. Public Concerns Regarding TSA Use of FRT

Civil society groups, privacy advocates, and legislators have expressed persistent concerns about TSA's use of FRT, including the potential for government use of FRT to expand beyond the scope of aviation security, such as to law enforcement or immigration enforcement, potential use for widespread surveillance, potential demographic differentials and their impacts, limited publicly available evidence of the need for these programs, and the potential chilling effect its use may have on Americans' civil liberties.[140] Some legislators have responded to these public concerns by introducing bills in Congress to restrict or eliminate the use of FRT by TSA and other federal government agencies.[141]

B. The Sensitivity of Biometric Data and Technologies

In this subsection, we discuss issues associated with FRT and biometric data generally without connecting all of them to the specific FRT applications in aviation at issue in this report. We provide this section for general context. These issues may not arise in every use of FRT; indeed, they may not arise in TSA's use of FRT as discussed in this report. In subsequent sections, we discuss TSA's specific use of FRT and ways in which TSA's current FRT program mitigates or avoids many of these risks.

Biometric data is a form of "personally identifiable information," or PII. DHS defines PII as "any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department."[142] PII includes information such as name, address, and phone number.

[140] *See, e.g., supra* note 52; *Digital Justice Initiative Comments to PCLOB Facial Recognition Roundtable*, *supra*; Elec. Priv. Info. Ctr., *Letter to PCLOB* (Jan. 27, 2020), https://epic.org/wp-content/uploads/privacy/facerecognition/PCLOB-Letter-FRT-Suspension.pdf.

[141] *See, e.g.*, Traveler Privacy Protection Act of 2023, S.3361, 118th Cong. (2023); Facial Recognition and Biometric Technology Moratorium Act of 2023, S. 681, 118th Cong. (2023); Facial Recognition and Biometric Technology Moratorium Act of 2023, H.R. 1404, 118th Cong. (2023); Ethical Use of Facial Recognition Act of 2020, S. 3284, 116th Cong. (2020).

[142] U.S. Dep't of Homeland Sec., *Handbook for Safeguarding Sensitive PII, Privacy Policy Directive 047-01-007*, at 5 (Dec. 4, 2017) https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20directive%20047-01-007%20handbook%20for%20safeguarding%20sensitive%20PII%2012-4-2017.pdf.

Sensitive PII (SPII) is a subset of PII and is defined by DHS as any information that could result in "substantial harm, embarrassment, inconvenience, or unfairness to an individual" if it is lost, compromised, or disclosed without authorization.[143] Some categories of PII qualify as SPII as stand-alone elements, meaning that they are sensitive regardless of whether such element is paired with any other identifier, including an individual's biometric identifiers (e.g., facial image), Social Security Number (SSN), and driver's license or state identification number. Other categories of PII can become SPII in conjunction with additional personal information, such as an individual's date of birth, citizenship or immigration status, and ethnic or religious affiliation.[144]

Facial images are unique in several ways. Unlike other types of SPII, an individual's face is not usually kept private; when you walk down the street, strangers can usually see your face. However, faces are nearly unique and adult faces rarely change. The use of FRT, in conjunction with databases containing personal information, can uniquely identify an individual, allowing the image to be linked to much more sensitive and non-public information.

DHS personnel are obligated by law and by DHS policy to protect PII to prevent identity theft or other adverse consequences, such as a privacy incident, compromise, or misuse of data.[145] SPII is subject to stricter handling guidelines beyond those used for PII due to the increased risks described above.[146] Recognizing facial images as SPII, as DHS does, helps to mitigate these risks.

[143] *Id.* at 5; Dep't of Homeland Sec., *DHS Sensitive Systems Policy Directive 4300A*, at 68 (July 27, 2017), https://www.dhs.gov/sites/default/files/publications/Sensitive%20Systems%20Policy%20Directive%204300A.pdf.

[144] *Handbook for Safeguarding Sensitive PII, Privacy Policy Directive 047-01-007*, *supra,* at 6.

[145] *See* Homeland Security Act of 2002, 6 U.S.C. § 142 (requiring the DHS Chief Privacy Officer to "assur[e] that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information" and to "assur[e] that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974"); Off. of Mgmt. and Budget, Exec. Off. of the President, *OMB Circular A-130*, *Managing Information as a Strategic Resource* (2016), https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf ("Agencies shall have comprehensive privacy programs that ensure compliance with applicable privacy requirements, develop and evaluate privacy policy, and manage privacy risks."); *see also Handbook for Safeguarding Sensitive PII, DHS Privacy Policy Directive 047-01-007*, *supra,* at 3; U.S. Dep't of Homeland Sec., *DHS Privacy Policy Guidance Memorandum 2017-01*, at 9 (Apr. 25, 2017), https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf; *DHS Privacy Policy Guidance Memorandum 2008-01*, *supra*, at 3.

[146] *Handbook for Safeguarding Sensitive PII, DHS Privacy Policy Directive 047-01-007*, *supra,* at 5. For example, DHS policy states that only those with an official need-to-know may access or use SPII; that databases that store SPII should employ technical safeguards and access controls to restrict access to staff with an official

1. Aggregation of Sensitive Data

To evaluate the risks of federal government use of biometric data, we must consider several types of information about individuals and how those types of information may be used and combined. First, traditional biographic data includes data about a person's identity such as name, address, date of birth, or SSN. Second, biometric data includes records of physical characteristics such as facial images, fingerprints, and iris prints. Third, there is information that may be revealing of an individual's activities, beliefs, and relationships.

Biographic and biometric information about individuals can be combined and linked in *biometric databases.* Law enforcement and administrative elements of the federal government, state governments, and third-party companies such as data brokers have already assembled instances of biometric databases that contain linked records of personal images and identity.[147] Most driving-age residents of the United States have a driver's license, meaning that a state registry of motor vehicles has a record containing an image of their face, their name, address, date of birth, other personal data, and often SSN.[148] The federal government maintains many databases that incorporate both biometric information (e.g., facial images, fingerprints, or other uniquely identifying information) and associated biographic information. For example, the DHS Office of Biometric Identity Management (OBIM) maintains IDENT, a database that stores biometric data and connects it to biographic information to establish and verify identities. IDENT serves as the "central DHS-wide system for storage and processing" of biometric information for "national security, law enforcement, immigration and border management, intelligence, background investigations," and other applications.[149] IDENT receives data from various DHS components, as well as the Department of State, the Department of Defense, and state and local investigative agencies.[150] Other elements of the government maintain biometric databases, although they are beyond the scope of this report. Many people have publicly accessible social media or other web accounts that make available images of their face and at least some portions of

need-to-know; and that SPII may only be accessed, viewed, saved, stored, or hosted on DHS-approved, encrypted portable electronic devices, such as laptops, tablets, and smartphones, as well as encrypted government-issued USB flash drives, CDs, DVDs, and external hard drives. *Id.* at 12.

[147] *See, e.g., Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy, GAO-16-267, supra,* (describing FBI's NGI-IPS). The fact that such databases exist does not necessarily imply that they are accurate or complete, especially considering private vendors.

[148] As of 2023, 86.24% of the driving age population of the United States was licensed. U.S. Dep't of Transp., *Highway Statistics 2023* (Jan. 2025), https://www.fhwa.dot.gov/policyinformation/statistics/2023/pdf/dl1c.pdf.

[149] *DHS/NPPD/PIA-002 Privacy Impact Assessment for the Automated Biometric Identification System (IDENT), supra*, at 2.

[150] *See generally id*.

their identity, further increasing opportunities for government agencies or commercial entities to assemble linked biographic information and images.

Queries into these biometric databases may be of two types. In the first, *biometric retrieval,* biographic information is used to retrieve the associated biometrics ("show me the image of this individual"). In the second, *biometric search,* a biometric image is used to retrieve the associated biographic data ("tell me the name of the person in this image"). Biometric retrieval has been possible for many years; a state DMV or police agency can pull a driver's license record, including a photograph, given a name. Biometric search is increasingly available as well, both in government applications as well as by private corporations.

As a distinct category of information from biographics or biometrics, *biometric-derived records* are created as an output of a biometric search operation and record additional information about an individual. Even if newly captured biometric data (e.g., the live photo taken at the point of entry) is immediately deleted, the use of biometrics may create new records containing sensitive information about individuals, such as whether an individual was at a particular location at a particular time or whether this individual used biometrics to access a facility. These records can be used to infer further and potentially sensitive personal information, such as their participation in public protests, their movements and locations visited, and their association with other individuals. For this reason, the use of FRT capabilities in conjunction with a biometric database may pose a greater risk to an individual's privacy and civil liberties.

2. Increased Risks of Aggregating Biometric Data

The combination of individuals' biographic and biometric information in a searchable database increases the sensitivity of the aggregated data and increases the risk of harm to an individual if the information is compromised or misused. Aggregated biometric data is a target for bad actors who regularly seek access to the most sensitive information on Americans. The risk of biometric data being leaked or stolen is not theoretical. A 2019 cyber attack resulted in the loss of approximately 184,000 traveler images retained as part of a DHS facial recognition pilot.[151] According to the Office of Personnel Management (OPM), hackers stole at least 5.6 million sets of fingerprints held by the federal government in 2015 in an incident that resulted in the loss of sensitive data of approximately 21.5 million

[151] U.S. Dep't of Homeland Sec., Off. of Inspector Gen., *Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot, OIG-20-71,* at 7–8 (Sept. 21, 2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

individuals.[152] And in 2023 alone, federal agencies reported eleven major cybersecurity incidents resulting in the breach of data on an untold number of Americans.[153] As federal agencies or other organizations collect and aggregate biometric and other data, the risk of loss of that data increases.

Additional privacy and civil liberties concerns arise from the widespread use of biometric data as personal identifiers. An increasing number of systems, both government and private, use a facial image as a unique identifier, equivalent to the combination of a username and a password. In such an arrangement, it may be easier for impostors to obtain an individual's facial images and attempt to impersonate them to gain access to their devices or online accounts. While in the event of a traditional identity theft, a credit card or even SSN can be revoked or reissued, a biometric identifier cannot, leaving individuals with little recourse or remedy.

Finally, the above-described risks of biometric databases assume that an individual's images and information are accurate and correctly attributed. Having a more complete record for an individual increases the likelihood that individual can be correctly identified. However, if any part of the data is incorrect, the individual may be falsely identified or may not be identified, potentially affecting that individual's ability to access benefits, flagging them for secondary investigation, or associating them with derogatory information.

As the use of biometric databases and biometrics as identifiers increases, the impact of incorrect or misattributed data will increase as well.

3. Distinctive Attributes of Facial Recognition

Facial recognition technology has several distinctive attributes that affect the kind and scope of privacy risks that its use can generate. First, labeled photographs are now widely available on the web, on social media platforms, and in certain government databases. This means that it can be relatively easy to accumulate large numbers of images that can be used for matching.

Second, capturing an image to match against these stored photos is relatively simple. Some facial recognition systems have specific requirements for images that can be used to match (e.g., the image must be squarely head-on, at eye level, well-lit); however, these

[152] Off. of Personnel Mgmt., *Cybersecurity Resource Center, Cybersecurity Incidents*, https://www.opm.gov/cybersecurity-resource-center/#url=Cybersecurity-Incidents (last visited Apr. 10, 2025).

[153] Exec. Off. of the President, *Federal Information Security Modernization Act of 2014 Annual Report, Fiscal Year 2023,* at 20 (June 2024), https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/06/FY23-FISMA-Report.pdf.

requirements are easing as technology improves. Unlike fingerprints, image acquisition requires no specialized equipment and can be done quickly at a distance. Face capture is efficient and may provide a touchless (i.e., more hygienic) alternative to other identity verification technologies; it also means that a photo can be captured and matched without the consent or even knowledge of the subject.

Third, because the process is performed largely by software, both capturing the image and attempting to match the image to one in the gallery can be automated and performed rapidly. This also increases the efficiency and speed of the system, while also suggesting the potential ability of FRT systems to perform surveillance in large public spaces.

Finally, unlike human attempts to match a subject in front of them with a document, automated facial recognition systems can attempt to match an acquired image with a very large set of potential matches if a 1:N system is employed. This may increase the risk that such systems could misidentify one subject as another, including potentially as someone sought by the authorities.

C. Comparison of Human and FRT Performance

In many contexts where FRT is deployed (such as with the TSA program discussed in this report), the technology serves to augment or replace humans working to verify or determine identities. Therefore, when considering the performance and accuracy of such systems, it is necessary to compare the performance of the technology with that of humans in the same context. Specifically, an important consideration for evaluating TSA's FRT systems is the relative accuracy of FRT systems compared to the human TSOs who would otherwise attempt to match travelers' faces to identification documents at security checkpoints. Indeed, relative accuracy rather than FRT's absolute accuracy is a key factor on which TSA's systems should be judged. TSA has not performed a study that directly compares the performance of TSOs with CAT systems, nor have academic or research studies performed tests precisely analogous to face matching at security checkpoints. Available studies suggest, however, that in similar contexts FRT is at least as accurate as, and very likely superior to, human performance.

It can be difficult to perform a direct comparison between the performance of humans and algorithms at face matching.[154] Relative performance can vary considerably depending on the difficulty of the comparison. For example, two images of the same person may differ due to aging, hairstyle, facial expression, and other physical variances; the more differences, the more difficult it is to perform a comparison. Additionally, environmental and

[154] Further, performance of FRT systems may differ from the performance of their underlying algorithms, as discussed above.

photographic quality factors, such as the angle of the image, the lighting, and the resolution, can make performing accurate comparisons challenging. Humans and algorithms find some of these varying factors challenging to a different degree; that is, some scenarios (e.g., images taken from an oblique angle rather than straight on) cause humans relatively little challenge, while FRT algorithms have historically struggled; others, such as different hairstyles, might confound humans but cause little difficulty to algorithms.[155]

Attempting to produce a simple comparison of FRT performance to human performance is also difficult because individual humans demonstrate a wide range of performance on face matching tasks. One study found the accuracy of face matching performed by passport examiners, who match faces as part of their professional duties, to range between lower than 60% to approximately 95%.[156] Even in a test that allowed three months to compare facial images, face examiners and similar professionals received accuracy scores between 0.5 (no better than chance) and 1.0 (perfect), with median performances of above 0.85.[157] There is mixed evidence of whether training can improve this performance. One review found that "[r]eports of effective training for unfamiliar face matching tasks are rare …. However, we have shown in recent work that face matching performance can be improved by some types of training."[158] Finally, it has been established that humans are better at matching familiar faces than unfamiliar ones,[159] and more accurately recognize individuals of their own race relative to other races (sometimes known as the "other-race effect").[160]

In the available reports that compare human performance to situations similar to that of TSA identity verification (e.g., well-lit, straight-ahead comparisons with high-quality reference photos), algorithms consistently showed higher performance. Even in 2012, tests found that "machines were never less accurate than humans on … challenging frontal

[155] For a broad review of factors influencing human performance, *see* Amy N. Yates et al., *Perceptual Expertise of Forensic Examiners and Reviewers on Tests of Cross-Race and Disguised Face Identification and Face Memory*, APPLIED COGNITIVE PSYCHOL. (Dec. 4, 2023), https://onlinelibrary.wiley.com/doi/epdf/10.1002/acp.70002.

[156] David White et al., *Passport Officers' Errors in Face Matching*, at Fig. 3 (Aug. 18, 2014), https://doi.org/10.1371/journal.pone.0103510 [hereinafter White 2014].

[157] P. Jonathon Phillips, et al., *Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms*, PROCEEDINGS OF THE NAT'L ACAD. OF SCI., at 6173, Fig. 2 (Apr. 30, 2018), https://www.pnas.org/doi/epdf/10.1073/pnas.1721355115.

[158] White 2014, *supra,* at 1.

[159] *Id*.

[160] *See* Alice O'Toole et al., *Predicting Human Performance for Face Recognition*, at 293–319 (2006), https://personal.utdallas.edu/~herve/abdi-ojra06-pretty.pdf.

images."[161] As described above, FRT algorithms have continued to improve in performance over the past decade. Given the current state of performance of the best algorithms, which can achieve 99% accuracy for straight-on, well-lit comparisons to high-quality reference photographs, there is little doubt that algorithmic systems are more accurate than typical humans. Given humans' own lower accuracy at performing face matching for demographic groups other than their own or for unfamiliar faces, FRT systems very likely surpass human performance even considering demographic differential performance of such systems.

D. Challenges in Performing Oversight on Projects in Development

TSA's use of FRT has evolved in significant ways since the early test deployments. For example, TSA has referred to its use of FRT as a "proof of concept" or "pilot" in 2018 and extending at least through 2025 for some aspects of the program.[162] CAT-2 production systems, which include 1:1 recognition capability, reached operational status in March 2024.[163] The nature of evaluating recently deployed programs or programs in development (i.e., prior to a formal decision to proceed with acquisition and deployment) raises certain challenges in performing fair, accurate, and comprehensive oversight.

First, by their nature, projects in development change over time as technology and systems improve and as an organization learns from its initial tests and refines or adjusts its approach. Consequently, evidence and records about the program may be accurate or meaningful only for certain stages of development, making it more difficult to draw conclusions about the program in general. It can be unclear during the development stage how exactly the program will operate when it is ultimately deployed and operational. The policy analysis and conclusions below are based on our best understanding of how these systems will operate when deployed and operational, but our analysis may change if TSA alters the program.

Second, oversight projects typically consider evidence establishing how a program contributed to an organization's mission, assessing the value, efficiency, and effectiveness of

[161] Alice J. O'Toole et al., *Comparing Face Recognition Algorithms to Humans on Challenging Tasks*, at 1 (2012), https://dl.acm.org/doi/10.1145/2355598.2355599.

[162] *See, e.g.,* U.S. Dep't of Homeland Sec., *Implementation of DHS Directive 026-11: Use of Face Recognition and Face Capture Technology, 2024 Report on Select Use Cases*, at 39, 41 (Jan. 17, 2025), https://govwhitepapers.com/whitepapers/implementation-of-dhs-directive-026-11-use-of-face-recognition-and-face-capture-technologies [hereinafter *Implementation of DHS Directive 026-11*] ("The TSA PreCheck: TIS [Touchless Identity Solution] is a "proof of concept" that is being assessed at specific airports with select airline partners." . . . "This technology is still in a field assessment phase. This means that it isn't fully operational.").

[163] PCLOB Fourth Round of Questions for TSA (Feb. 2024). Formally, DHS refers to this stage of an acquisition program as an Acquisition Decision Event 3 (ADE-3). CAT-2 ADE-3 Increment 1 ADM, *supra*.

the program, and evaluating compliance incidents or other indications of harm. Such a comprehensive record does not yet exist for programs in development or for programs that were only recently deployed. As a result, oversight of recent programs or programs in development must instead rely on plans and design goals rather than past performance, and limited results from early tests and assessments which might be derived from configurations of the system different from the ones ultimately deployed.

Below, in Section IV.A. below, we discuss issues associated with transparency and disclosure relating to how TSA characterized its development program.

II. EFFECTIVENESS AND VALUE

TSA's use of FRT at checkpoints to determine the identity of travelers is part of its broader efforts to promote aviation security. To evaluate the effectiveness and value of the program, we consider the role played by FRT within TSA's security mission; the accuracy of the algorithmic comparison; the impact of using FRT in place of officers' comparison of faces to images in identity documents; and the ability of the system to detect or prevent impostors from passing through the checkpoint, especially as compared to human officers. As described above, it is challenging to evaluate the effectiveness of a program in development, as a full record of results is not yet available. However, we can draw certain conclusions from initial results and comparable results from related systems or testing.

A. Contribution to TSA's Mission

TSA's mission is "to protect the Nation's transportation systems and to ensure freedom of movement for people and commerce."[164] In the aviation context, TSA's responsibilities include securing aviation transportation, conducting screening operations for passenger air transportation, assessing threats to transportation, and coordinating countermeasures.[165] The deployment of biometrics has the potential to improve both security effectiveness and operational efficiency.[166]

1. Security Effectiveness

Confirming the identity of travelers is a key part of TSA's risk-based aviation security model.[167] TSA has asserted that evolution in techniques used by impostors and the use of fraudulent identity documents, combined with rising volumes of air travel, have exacerbated limits of manual identity checks to operate effectively or in a timely fashion.[168]

Before the launch of the FRT pilot programs, TSA relied solely on TSOs to confirm that passengers matched the photo on their identity document. Unless a traveler chooses to opt out, TSA currently uses FRT at many checkpoints to perform that matching function. By

[164] *See* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *SIDA Airport Security, Fiscal Year 2017 Report to Congress*, at 2 (Feb. 6, 2018), https://www.dhs.gov/sites/default/files/publications/TSA%20-%20SIDA%20Airport%20Security.pdf.

[165] 49 U.S.C. § 114(d)–(f).

[166] *See, e.g.,* Biometrics Roadmap, *supra,* at 6.

[167] *DHS/TSA/PIA-046(d) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, *supra*, at 6; Letter from David Pekoske, Administrator, Transp. Sec. Admin., to Sen. Jeff Merkley (D-OR), at 1 (May 17, 2023).

[168] U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *TSA Response to Sen. Jeff Merkley (D-OR) Questions in February 9, 2023, Letter* (May 17, 2023).

establishing that travelers match their identity documents (or images associated with their enrollment in Trusted Traveler Programs), TSA states it has more confidence that it is successfully preventing people identified as potential dangers from entering the boarding area of the airport. This prevention is accomplished primarily through TSA checking travelers' biographic details against information in the Terrorist Watchlist. TSA FRT systems do not compare facial images collected at security checkpoints (i.e., through 1:1 or 1:N systems) against the Terrorist Watchlist.

FRT-enabled identity authentication may serve as a deterrent to malicious actors attempting to fly. It is, of course, difficult to measure the impact of such deterrence directly. Similarly, it is presently unknown to what extent TSA's use of FRT may have prevented terrorist attacks or travel. Similar points apply to the previous identity authentication system, making a direct comparison difficult.

The ability of CAT devices to detect fraudulent identity documents does not rely on the use of FRT; TSA's 1:1 system uses FRT to determine whether the image captured of the person presenting the identity document is sufficiently similar to the image on the document.[169] For example, a fraudulent identity document may contain an actual image of the holder. In such a case, FRT would correctly report a match between the holder and the document. A separate inspection process can determine that the document itself was illegitimate (e.g., using improper formatting, lacking a holographic seal, or other indications that the document does not conform with standards for that document type). The CAT device performs this document inspection process, though a TSO may perform further inspection manually, depending on the results from the CAT device shown to the TSO.[170]

2. Operational Efficiency

The shift to FRT likely makes the identity and boarding pass verification process more efficient. However, there is not yet comprehensive data showing the impact of the use of FRT on overall security checkpoint efficiency, including physical and baggage screening.

FRT provides a near real-time matching of the ID photo to a recently captured image, thus improving the efficiency of determining traveler identity.[171] For the 1:N pilot, TSA has

[169] *See DHS/TSA/PIA-046(b) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Verification*, *supra,* at 3. TSA's 1:N system does not inspect or validate identification documents at the checkpoint, relying instead on previous authentication of individuals as they enrolled in TSA PreCheck or other Trusted Traveler Programs. *See TSA Precheck® Touchless ID, supra*.

[170] *See DHS/TSA/PIA-046(d) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, *supra*, at 3–4; *see DHS/TSA/PIA-046(b) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Verification*, *supra*, at 4.

[171] TSA Responses to Third Round of PCLOB Questions (Dec. 2023).

stated that it takes approximately 10 seconds per traveler transaction—including face image capture, data transmission to CBP TVS, matching to the airport-specific day-of gallery, validating against Secure Flight, and transmission of that response back to the TSO—for the TSO to make a final decision.[172] During TSA's assessment of 1:N, TSA processed more than 400 travelers an hour, compared to approximately 180 travelers an hour using manual verification.[173] TSA has not provided equivalent metrics for 1:1 processing, as TSA does not track processing times for 1:1 matching.

Increased photo matching speed may provide advantages for workforce demands (e.g., reducing the number of TSOs required to validate documents) and may allow travelers to enter the physical screening portion of the checkpoint more quickly. TSA has acknowledged, however, that "the operational efficiencies TSA could gain from integrated biometric solutions may be different depending on airport facility layouts, sizes, checkpoint lane counts, and traveler volumes."[174] At some checkpoints, for example, faster photo-matching could merely shift passengers into longer lines at physical screening, while at other checkpoints use of FRT could free TSOs to staff other parts of the screening process.

During TSA's assessment of 1:N, TSA processed more than 400 travelers an hour, compared to approximately 180 travelers an hour using manual verification.

TSA's previous method of identity verification involved a TSO visually inspecting a traveler's boarding pass and physical ID for matching traveler information and appearance, as well as inspecting the documents for indications that those documents may be fraudulent.[175] According to TSA, the use of FRT reduces TSOs' primary screening burden of reviewing and verifying 2.5 million travelers daily and allows them to focus on secondary alert resolutions.[176] TSA states that the FRT system allows a TSO to focus more attention on a subset of alerts for particular documents or people.[177]

[172] *Id.*

[173] *Id.*

[174] U.S. Dep't of Homeland Sec., Transp. Sec. Admin. & Customs and Border Prot., *Deployment of Biometric Technologies Report to Congress*, at 16 (Aug. 30, 2019).

[175] TSA Responses to Third Round of PCLOB Questions, (Dec. 2023).

[176] *Id.*

[177] *Id.*

3. Detecting and Deterring Security Threats

The applicability and effectiveness of FRT in a security context depends on its ability to identify unauthorized travelers. In one scenario, the traveler is using their own authentic identity document. Standard security measures (e.g., Secure Flight or identity document review) should identify the individual. Personnel should then respond appropriately, such as by denying boarding or having the traveler undergo enhanced screening. The use of FRT could be beneficial in this scenario by more accurately matching the individual to the identification document, compared to matching by manual inspection. As a secondary effect, this capability may cause terrorists to be more cautious about traveling using U.S. airlines and to avoid travel or resort to less-convenient modes of travel. Like any counterterrorism measure that results in potential terrorists employing less-desirable methods, this could be part of an effective strategy to deter individuals from travel aboard U.S. airlines or through U.S airports. Due to the increased speed of FRT-based identity determination, TSOs have more time to inspect carefully other travelers, such as those who do not match.[178]

In a second scenario, the traveler is unlawfully traveling using someone else's authentic identity document. If this alternate identity document belongs to an individual who has not been identified by the government as being of concern (perhaps obtained cooperatively or through identity theft), FRT may detect that such impersonation is occurring by correctly determining that the traveler's face does not match the image of the legitimate individual on the identification document.

In a third scenario, the traveler attempts to use a fraudulent or forged identification document that contains their actual image. In such a case, FRT would correctly report that the traveler matched the image. However, in addition to their FRT capabilities, CAT devices (of either generation) attempt to authenticate identification documents and can recognize many forms of fraudulent documents.

Malicious actors can attempt to defeat FRT in the above scenarios, for example by wearing a disguise face mask;[179] intentionally choosing an individual to travel who looks very similar to the person in an authentic identity document; or generating an identity

[178] For a discussion about the importance of deterrence and prevention in the broader context of aviation security strategy, *see* U.S. Dep't of Homeland Sec., *National Strategy for Aviation Security,* at 12–13 (March 26, 2007), https://www.dhs.gov/sites/default/files/publications/nspd-47.pdf.

[179] The use of disguise face masks, usually made of flexible silicone, to fool FRT systems is known as a type of "presentation attack." *See, e.g.,* Matineh Pooshideh et al. *Presentation Attack Detection: A Systematic Literature Review*. ACM COMPUTING SURVEYS 57, 1, Art. 25 (Oct. 2024). https://doi.org/10.1145/3687264.

document that contains a "morph" image that combines images of multiple people, such that they potentially fool FRT systems into accepting either individual as a match.[180]

In both 1:1 and 1:N modes, the consequences of false positives due to impostors imply a potential security threat; someone lying about their identity has successfully passed through the security checkpoint. This means that TSA and DHS's pre-travel screening and risk assessment have been bypassed. This could include, for example, in a 1:1 context, an impostor who obtained a false identification document that showed their image.[181] In TSA's 1:N system, because only travelers enrolled in TSA PreCheck have images in the gallery, an impostor would need to have made a reservation using the identity of someone else enrolled in TSA PreCheck.[182]

For this reason, FRT systems used for access control, such as TSA's security checkpoint, are usually configured with a threshold for similarity that produces a very low false positive rate. However, overall false positive rates observed in testing do not necessarily reflect the threat of impostors. When testing for false positive rates, testers must decide how much effort to make to provide the system with difficult cases. In the easiest case, called zero-effort impostor detection, matches are attempted across the entire range of test subjects. However, most of those potential pairs are highly unlikely to generate a false match as the faces will be extremely distinct. Increasing amounts of effort might include only matching race (or nation of origin), gender,[183] age, or a combination of demographic attributes, in order to test the system's ability to distinguish more similar (but not identical) facial images.

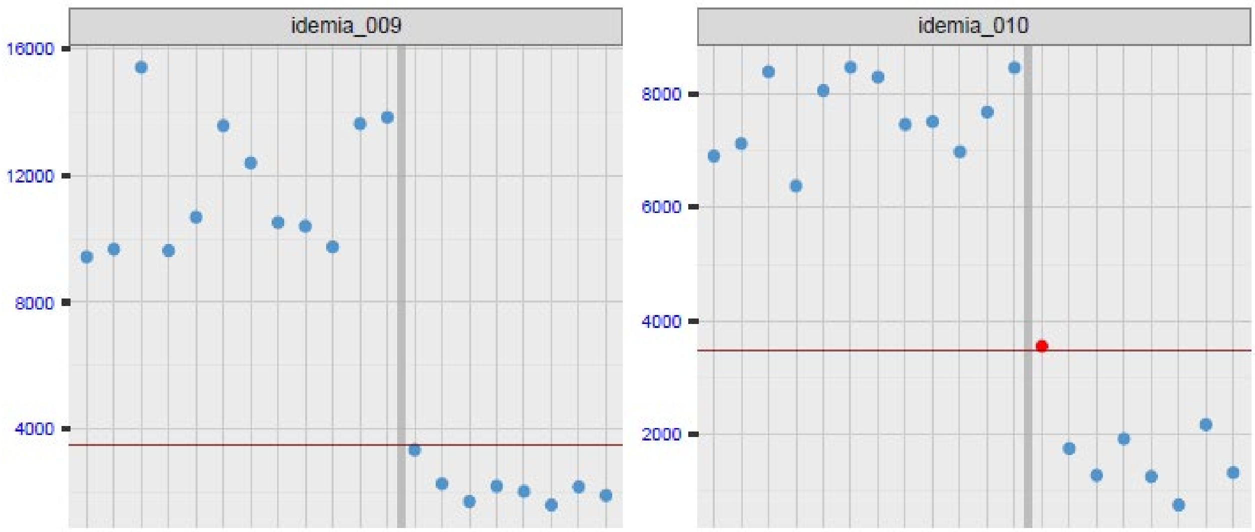
[180] *See generally* Mei Ngan et al., *NISTIR 8292 Draft Supplement, Face Analysis Technology Evaluation (FATE) Part 4: MORPH - Performance of Automated Face Morph Detection*, NAT'L INST. OF STANDARDS AND TECH. (Feb. 27, 2025), https://pages.nist.gov/frvt/reports/morph/frvt_morph_report.pdf.

[181] Note that fraudulent identification does not necessarily imply terrorist or violent intent; it may merely be an individual seeking to use someone else's ticket.

[182] Alternately, a would-be impostor could hope to randomly match to another traveler in the gallery. Such an approach would be unlikely to succeed, and would be detected if the legitimate traveler had already passed through the checkpoint, or would be detected later (and perhaps too late) if the legitimate traveler arrived after the impostor.

[183] The majority of academic and technical research and testing on demographic effects in FRT have used the term gender, and thus we use that word to describe the results of such research. *See, e.g.,* NAS FR Report, *supra.* When describing federal government policies and procedures, we use the term "sex" consistent with current Executive Branch policy. When characterizing the contents of historical documents or publications, we use the term in the source material. *See* note 48, *supra.*

In one test NIST performs to evaluate the ability of an algorithm to detect impostors, NIST uses a set of 20 pairs of images (12 genuine and 8 impostor images) specifically selected for difficulty. In that test, idemia_009 correctly identified all 20 pairs, and idemia_010 identified all genuine pairs correctly and 7 out of 8 impostor pairs. The following diagram shows the similarity score calculated by the algorithms for true matches (on the left-hand side of each graph) and impostor pairs (on the right-hand side of each graph).



Above: This chart shows algorithms' similarity scores for 12 genuine and 8 impostor image pairs. The threshold (red horizontal line) is a value calibrated to give a false positive rate = 0.0001 on mugshot images. Points above the threshold correspond to pairs determined to be genuine, and points below the threshold correspond to pairs determined to be impostors. If the determined class (genuine or impostor) matches the real class, points will be blue; if not, red.[184]

CBP, which uses TVS at border ports of entry, reports that of the 697 million travelers that it has processed using FRT, it has detected more than 2,100 impostors (i.e., individuals using genuine travel documents that do not match their identity) attempting to enter the United States.[185] Because it is unknown how many impostors escaped detection, it is impossible to estimate the precise effectiveness of the system in detecting impostors. TSA has not provided results of any real-world studies or tests regarding their FRT systems' ability to detect potential impostors.

[184] Nat'l Inst. of Standards and Tech., *Face Recognition Technology Evaluation (FRTE) 1:1 Verification*, at 183, Fig. 38 (March 18, 2025), https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf.

[185] U.S. Dep't of Homeland Sec., Customs and Border Prot., *Biometrics: Locations; Where is CBP Using Biometrics Today?* https://www.cbp.gov/travel/biometrics/locations (last visited Apr. 15, 2025).

B. Testing and Performance Characteristics

A core characteristic of TSA's FRT system that influences effectiveness is the extent to which the system is able to determine the identity of travelers accurately, whether by validating that they match their presented identity document (i.e., using 1:1 recognition) or by matching them to the correct image in a gallery of expected travelers (i.e., using 1:N identification). There have been multiple types of evaluation of the accuracy of system components. This includes algorithmic testing by NIST, a simulated test performed by NIST using TSA and CBP operational data,[186] scenario testing by DHS S&T, and other testing and evaluation performed by TSA and DHS S&T during the acquisition process. Since the program's inception, neither TSA nor independent researchers have assessed the operational success of the system as deployed. Some aspects of such an operational evaluation could be difficult to interpret. Standard operational testing could collect data on efficiency and false negative rates, for example. However, collecting accurate statistics on false positive rates (e.g., successful impostors) would be difficult, as by definition they escaped detection. Measuring the ability of impostors to pass through the TDC stage of a checkpoint requires some form of adversarial testing.

In this section, we focus on the overall rates of false positives and false negatives and their implications for system efficacy.

1. <u>NIST Algorithmic Testing and Evaluation</u>

IDEMIA has submitted multiple algorithms to NIST's FRTE. For the most recent version of IDEMIA's 1:1 algorithm submitted to NIST (idemia-011, submitted August 6, 2024), the false negative rate (that is, the rate at which the system incorrectly reported that a new image of an individual did not match a reference photograph of that same individual) ranged from 0.18% to 0.77% for use cases similar to the use by TSA.[187] Idemia-011 achieved the 5th best false negative rate, in the top 2% of results, when comparing high quality photographs, and

[186] NIST simulated the operations of FRT in an airport by using CBP entry and exit photographs to construct simulated flights of 400 random people and attempted to perform face matching between the pairs of photos. Nat'l Inst. of Standards and Tech., *NISTIR 8381 Draft Supplement, Face Recognition Vendor Test (FRVT) Part 7: Identification for Paperless Travel and Immigration*, (Oct. 28, 2021), https://pages.nist.gov/frvt/reports/travel/frvt_travel_report.pdf; *see also* Nat'l Inst. of Standards and Tech., *FRTE Paperless Travel*, https://pages.nist.gov/frvt/html/frvt_paperless_travel.html (last visited Apr. 15, 2025).

[187] Nat'l Inst. of Standards and Tech., *Face Recognition Technology Evaluation (FRTE) 1:1 Verification*, https://pages.nist.gov/frvt/html/frvt11.html (last visited Dec. 17, 2024). These tests varied in the quality of probe and reference photographs and in the threshold used to control the level of false positives.

the 48th best false negative rate, in the top 13% of results, when comparing low-quality photographs.[188] False positive rates ranged from 0.0001% to 0.001%.

In NIST testing of the most recently submitted version of NEC's 1:N FR algorithm (nec_010, submitted January 24, 2025), false negative rates for comparable scenarios ranged from 0.07% to 4.4% depending on gallery size, quality of gallery photographs, quality of live images, and age of the gallery photographs.[189] These results ranked among the top three algorithms (of 135) for all tests. For these tests, NIST configured the threshold to produce a false positive rate of 0.3%.[190]

In 2021, NIST performed a series of tests meant to simulate the use of 1:N facial recognition in air travel (so-called "paperless travel").[191] This test used actual photographs of travelers collected by DHS OBIM at airport border control entry and exit and measured algorithms' ability to correctly match exit photographs against galleries of entry photographs. To simulate the use in aviation security, NIST assembled galleries of 420 individuals representing notional flights; NIST also tested a mode of 42,000 individuals, representing a more centralized security model. The threshold was set at a value that produced a false positive rate of 0.03%.

NIST continued running these tests with updated versions of algorithms submitted by vendors through January 23, 2023.[192] The most recent version of the 1:N algorithm from NEC submitted to NIST prior to that (nec-005, submitted December 13, 2021) failed to recognize

[188] *Id.* At the time the data was queried for this report, there were 377 algorithms in the comparison.

[189] More specifically, nec_010 had a false negative identification rate (FNIR) of 0.07% for mugshot-to-mugshot (M2M) comparisons with a gallery size of 12 million; a 0.06% FNIR for M2M comparisons with a gallery size of 1.6 million; a 0.57% FNIR for mugshot-to-webcam comparisons with a gallery size of 1.6 million; a 0.15% FNIR for a comparison of visa photographs with photographs taken at the border with a gallery size of 1.6 million; a 4.4% FNIR comparing visa photographs with images taken at a kiosk with a gallery size of 1.6 million; a 0.52% FNIR for comparison of photographs taken at the border with photographs taken at the border more than 10 years previously, with a gallery size of 1.6 million; and a 0.19% FNIR for a comparison between mugshot images and mugshot images more taken more than 12 years previously, with a gallery size of three million. FNIR rates varied in these tests because they stress the ability of the system to identify matches in different ways. *See* Nat'l Inst. of Standards and Tech., *Face Recognition Technology Evaluation (FRTE) 1:N Identification*, https://pages.nist.gov/frvt/html/frvt1N.html (last visited Apr. 15, 2025).

[190] *Id*.

[191] Nat'l Inst. of Standards and Tech., *NISTIR 8381, Face Recognition Vendor Test (FRVT) Part 7: Identification for Paperless Travel* (July 2021), https://github.com/usnistgov/frvt/blob/nist-pages/reports/travel/frvt_travel_report_2021_07_12.pdf.

[192] NIST released the latest version of the paperless travel report on October 28, 2021, but continued to update the website with results. The most recent vendor submission was June 7, 2022, and NIST closed the FRTE paperless travel project on January 23, 2023. *See* Nat'l Inst. of Standards and Tech., *FRTE Paperless Travel*, https://pages.nist.gov/frvt/html/frvt_paperless_travel.html (last visited Apr. 15, 2025).

travelers 0.18% of the time when using galleries of 420 individuals, where each individual appeared in the gallery only once. When multiple images of travelers were included in the galleries, the false negative rate fell to 0.08%. For galleries of 42,000, nec-005 experienced a false negative rate of 0.32%.[193]

2. TSA and DHS S&T Testing

DHS S&T and TSA have evaluated the performance of the FRT in the CAT-2 systems. In early 2020, DHS S&T evaluated the accuracy and performance of the version of the CAT-2 system in existence at that time. At the threshold value DHS S&T selected for testing, the system showed a false positive rate of 0.17%.[194] The system failed to make a comparison 5.8% of the time, either because it could not acquire a live image (2.1%) or did not acquire an image from the document (3.7%).[195] The system had a false negative rate of 3.8%.[196] Tests also showed that the false positive rate varied by the type of identity document used, with notably higher false positive rates for U.S. passports (0.21%) relative to driver's licenses (0.17%).[197] Later testing in 2023 found that the system correctly matched 99.4% of participants, and 99.9% of those participants for whom the system successfully acquired both a live image and the image from their presented identification document.[198] See Section III.C. below, for a more detailed description of findings from this test.

In testing done by TSA in 2023, for travelers processed using 1:1 matching, TSA found that the "true acceptance rate" (that is, the proportion of all attempts that correctly matched the traveler image to the image on the identity document) was 99.3%, and the false positive rate was lower than 1 in 250.[199] However, TSA stated that it does not capture metrics for the number of travelers who opt out, the number of travelers successfully processed using 1:1

[193] *Id.*

[194] SAIC Identity and Data Sciences Lab. at the Maryland Test Facility, *Field Site Efficacy Evaluation: TSA CAT-2 Pilot Interim Biometric Assessment*, at ii (March 2020).

[195] *Id.* at iii. At the time of the report, DHS S&T informed PCLOB that it had not determined explanations for why the system failed to acquire images from documents. This may be addressed in later investigations or testing.

[196] *Id.*

[197] *Id.*

[198] U.S. Dep't of Homeland Sec., Science and Tech. Directorate, *Credential Authentication Technology (CAT2): Demographic Differentials in Biometric Performance* (Feb. 2024) [hereinafter DHS S&T 2024 Demographic Study].

[199] TSA Responses to Fourth Round of PCLOB Questions (Feb. 2024) (citing System Evaluation Report for the CAT-2 Upgrade Kit (May 1, 2023)). Note that TSA considers the exact false positive rate to be SSI and does not disclose it to the public.

matching, or the number of travelers processed using 1:1 matching who were discovered to be using fraudulent identification.[200]

In February 2024, TSA and DHS S&T found that, for travelers processed using 1:1 systems, the face capture success rate and the face matching success rate were more than 99% accurate, both of which did not vary based on age, gender, race, or skin tone.[201] Additionally, DHS found that, on average, the TSA CAT-2 identity verification process took 22.8 seconds per person and under 30 seconds for all demographic groups.[202] The demographic differentials found in this scenario testing will be further described in Section III.C.

In the fall of 2024, using both scenario testing and operational data, TSA and DHS S&T found that, for travelers processed using 1:N matching, the technology was more than 99% accurate for all demographic groups.[203] The demographic differentials found in this scenario testing will also be further described in Section III.C.

3. Ongoing Development and Testing

IDEMIA and NEC, like most FRT algorithm developers, continuously refine and update their algorithms. Most often, these updates achieve more accurate results; however, demographic differentials may exist for specific subgroups. TSA and DHS S&T regularly review updated versions of IDEMIA's algorithm and compare their performance on actual data against previous versions. DHS states that only updates that meet standards for accuracy and demographic differentials are incorporated into system updates.

C. Conclusion

The effectiveness and value of adding FRT capabilities into the airport security system are derived primarily from the system's accuracy and speed. TSA has taken several steps to ensure the accuracy of the identity verification process. The PII obtained from Secure Flight for CAT-2 use is the same information that the individual entered when booking their flight, and thus should be the same information that is on the identification document and boarding pass the traveler presents to TSA on the day of travel.

[200] TSA Responses to Fourth Round of PCLOB Questions (Feb. 2024).

[201] DHS S&T 2024 Demographic Study, *supra*.

[202] *Implementation of DHS Directive 026-11*, *supra,* at 36.

[203] *Id.* at 41.

The algorithms TSA has employed for 1:1 and 1:N FRT are extremely accurate when tested in ideal situations. While there are few direct comparisons, FRT is generally more accurate under typical conditions in a controlled setting; that is, FRT systems are more likely than humans to correctly identify that two images are, or are not, of the same person. To the extent that data is available showing performance for more realistic situations, both false positive and false negative result rates are still very low. These different types of errors matter for security in different ways. False positives represent an increased threat of impostors; for 1:1, they can only arise through impostor attempts, while for 1:N they can arise due to impostors or facial similarities between legitimate travelers. False negatives, on the other hand, primarily represent an inconvenience to the traveler, as described in further detail in the following section. However, to the extent that such false negatives slow down processing or require additional attention from TSOs, they can also impede the efficient functioning of the system.

FRT can perform comparisons of faces far faster than humans and is generally believed to be more accurate under typical conditions in a controlled setting. Whatever the effectiveness of TSA's larger security screening processes, the introduction of FRT is very likely to be a positive contribution to the accuracy and efficiency of TSA's ability to determine the identity of travelers compared to the previous system.

In addition, FRT can perform comparisons of faces far faster than humans. Therefore, whatever the effectiveness of TSA's larger security screening processes, the introduction of FRT is very likely to be a positive contribution to the accuracy and efficiency of TSA's ability to determine the identity of travelers compared to the previous system. However, because TSA does not have metrics on the number of impostors detected nor estimates of the number of impostors who are currently undetected, we are unable to evaluate the absolute contribution of the system to security or the cumulative effect of the entire passenger screening and authentication function.

III. Consequences of Misidentification and Demographic Impacts

Above, we discussed the impact that incorrect determinations by the FRT system have on security effectiveness. Here, we consider the additional consequences when FRT fails to recognize a legitimate traveler due to a failure to perform a matching operation (such as through failing to acquire an image or producing a false negative result) or mistakenly matches them to another traveler due to a false positive match arising in a 1:N scenario. Failures to perform a match operation result in the traveler requiring manual identity verification by the TSO. False positives may have unpredictable consequences. The traveler may be allowed to proceed, as the system (incorrectly) identifies them as a (different) legitimate traveler. However, if that other traveler has already passed through security, it may appear that the second traveler is an impostor.

A further concern, as described in more detail below, is that the occurrence of these errors, while low, is currently not uniformly distributed across demographic and personal attributes, and certain segments of the population may experience a disproportionate share of such errors and the resulting inconvenience. In this context, "demographics" encompasses a wide range of attributes, including age, national origin, gender, race, skin tone, and others, as well as the interactions and combinations of these factors.

A. Implications of Failed or Incorrect Identification of Travelers

If the FRT system does not establish a match, the TSO performs a manual review of the traveler's identification document.[204] This additional manual inspection does not require the traveler to move to a different line, nor does it affect the type of physical screening that the traveler will receive. Manual inspection of the identity document by the TSO takes only a few additional seconds. However, it may cause embarrassment or discomfort to the traveler, especially in the stressful environment of airport security checkpoints. Given the higher rates of fallibility of humans when compared to FRT, it is possible that the TSO may also incorrectly reject the match between the traveler and their identity document (e.g., if the picture on the identity document is a particularly low-quality image or poor likeness of the traveler).[205]

[204] *DHS/TSA/PIA-046(d) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, *supra*, at 3–4.

[205] For Real ID-compliant driver's licenses, states must follow the photo quality standards specified in ISO/IEC 19794-5:2005. 6 C.F.R. § 37.17(e)(1).

These individual inconveniences are multiplied by the very large number of travelers that pass through TSA security. In 2023, TSA screened more than 850 million travelers; travel volume in 2024 increased to more than 900 million travelers, a greater than 5% increase over the previous year.[206] A false negative rate of 0.2% of the FRT system on its own could cause more than 1.7 million travelers annually to fail to be initially identified as matches. However, in practice, TSOs will manually review any negative match results and allow through travelers who they determine match their identity documentation. Moreover, as discussed above, because we do not know the false negative rate for manual TSO face matching, we cannot say how the addition of FRT compares to the historical false negative rate. (See Recommendation 2, below, which addresses testing and red-teaming to measure this capability.)

B. Demographic Differentials

Currently, most FRT systems can exhibit different levels of accuracy for different demographic groups or attributes. That is, the false positive and/or false negative rates experienced by a particular FRT system may differ depending on the gender, age, race, or other physical attributes of the individual being matched.[207] This effect is often referred to as "demographic differential performance" or "demographic disparities." Which demographic groups are affected, and the magnitude of the difference, vary considerably between algorithms from different vendors, and are also affected by operational factors such as dirty lenses or variable ambient lighting. As described in more detail below, the algorithms from IDEMIA and NEC, the FRT suppliers used by TSA, show minimal demographic

[206] *Compare* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *2024 TSA checkpoint travel numbers*, https://www.tsa.gov/travel/passenger-volumes/2024 (last visited Aug. 16, 2024) *with* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *2023 TSA checkpoint travel numbers*, https://www.tsa.gov/travel/passenger-volumes/2023 (last visited Aug. 16, 2024).

[207] Iris recognition, a biometric identification technique in which infrared light is used to image an individual's unique iris pattern, has a low false positive rate. Testing at DHS S&T has concluded that, using the most common current algorithm, the performance and accuracy of iris recognition does not appear to depend on demographics. *See* Yevgeniy Sirotin & Arun Vemury, *Demographic variation in the performance of biometric systems: insights gained from large-scale scenario testing*, U.S. Dep't of Homeland Sec., Science and Tech. directorate, at 15, 20 (March 30, 2021), https://www.dhs.gov/sites/default/files/publications/21_0708_st_demographic_variation_performance_biometric_systems.pdf. The feasibility of implementing this technique is currently limited by the relatively small number of iris records available for matching, low capture rates, and improved ease of use of FRT compared with iris. The difficulty of obtaining live images can also lead to false negative results. However, TSA plans to test the use of iris scans, and this technique may provide an effective future system that does not suffer from demographic differentials. *See* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *TSA Myth Busters: Biometrics* (June 7, 2022), https://www.tsa.gov/sites/default/files/biometricsmythvsfacts_6_7_22.pdf.

differentials, measured in both absolute and relative terms, compared to other algorithms, although such differentials may still affect numerous travelers.

Although much attention has been focused on demographic differentials in the core face matching algorithms, differential performance can also be caused by other parts of the overall system. For example, there may be differentials in a system's ability to identify faces in images, and these may arise due to non-algorithmic factors such as cameras, lighting, and system usability. In practice, these may be the most important causes of demographic differentials.

The two FRT algorithms used by TSA show minimal demographic differentials, measured in both absolute and relative terms, compared to other algorithms, although such differentials may still affect numerous travelers.

Academic researchers, civil society groups, and journalists have raised concerns about demographic disparities in facial recognition and related technologies, especially around race and gender, for many years.[208] The NAS FR Report concluded that, despite improvements in overall performance of FRT systems, these demographic differentials have not entirely gone away, even among the most accurate systems.[209] Among its findings, it observed that "testing has demonstrated that [false positive] match rates for Black individuals and members of some other demographic groups are relatively higher (albeit low in absolute terms) in FRT systems that are widely used in the United States."[210] False positive rates also tend to be higher for women and older individuals.[211] These disparities occur even when both the live image and the reference images are of high quality.[212] As mentioned above, false positives generally do not inconvenience legitimate travelers, but may pose security issues.

[208] *See, e.g.*, Kashmir Hill, *Your Face Belongs to Us: A Secretive Startup's Quest to End Privacy as We Know It* (2023); Am. C.L. Union, *Face Recognition Technology*, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology; Joy Buolamwini, *Unmasking AI: My Mission to Protect What Is Human in a World of Machines* (2023).

[209] NAS FR Report, *supra*, at 3.

[210] *Id.*

[211] *Id.* at 56.

[212] *Id.* at 4.

One of the most comprehensive studies of demographic differential performance was the NIST's 2019 Face Recognition Vendor Test.[213] Five years later, the NIST demographic report remains informative.[214] Since the initial publication of this report, NIST has continued to update its measurements of demographic differentials in regular updates on NIST's website and in updates to the original report.

The 2019 NIST report found that demographic differentials vary widely by algorithm. Most algorithms that NIST tested had at least some observable demographic differentials; algorithms that were less accurate overall tended to have more pronounced differentials.[215] The degree of demographic differentials depended on whether an algorithm was performing 1:1 or 1:N matching and whether NIST was testing for false positives or false negatives. Generally, algorithms had higher demographic differentials in their false positive rate than their false negative rate.[216] As we said above, false negatives are more likely to inconvenience the traveler. A false positive would mean that an impostor would be more likely to pass through security undetected.

The NIST study tested 189 facial recognition algorithms not specifically in the context of airport security.[217] For most algorithms, the NIST study measured higher false positive rates in women, African Americans, and particularly in African American women. As mentioned above, false positives generally do not inconvenience legitimate travelers but may pose security issues. For some algorithms, these differentials ranged by a factor of 10 to 100.[218] However, NIST found that some 1:N algorithms gave similar false positive rates across these specific demographics. The NIST study found elevated false positives in the elderly and in children; the effects were larger in the oldest and youngest, and smallest in middle-aged adults. NIST also identified higher false positive rates with respect to race, identifying specifically Africans, African Americans, East Asians, and South Asians as groups that experience higher false positive rates.[219] However, with a number of algorithms developed in China the effect for East Asians is reversed, with low false positive rates on East

[213] *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280*, *supra*.

[214] *See* NAS FR Report, *supra*, at 56.

[215] *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280*, *supra,* at 2, 6.

[216] *Id*. at 2–3.

[217] *Id*. at 1.

[218] *Id*. at 2–3. Specific absolute false positive rates varied significantly between algorithms. A typical algorithm's performance was often in the range of a false positive rate of 0.01% (or 1 in 10,000) for white men, and 0.1% (or 1 in 1,000) for African American women.

[219] *Id*. at 7.

Asian faces.[220] This suggests that if the training dataset for an FRT algorithm is sufficiently representative of demographic groups, differential performance among them could be reduced. More recent academic research has continued to identify patterns of demographic differential performance of FRT systems.[221]

Patterns of demographic differentials in the core face comparison algorithms, and the causes of those differentials, vary significantly between false negatives and false positives. Differentials in rates of false negative errors, which primarily impact legitimate travelers and potentially burden TSOs, are relatively small; on the order of a factor of two or three between the demographic groups with the lowest rates and those with the highest rates.[222] False negative rates are substantially affected by image quality, particularly under-exposure of individuals with darker skin tones.[223]

Differentials in false positive error rates in the core face comparison algorithms are significantly higher; in many algorithms submitted for NIST testing in 2023, the false positive rate for demographic groups with the highest false positive rates is 1,000 times higher, or more than, the false positive rate for demographic groups with the lowest false positive rate.[224] Unlike false negative rates, false positive differentials occur even with the use of higher quality images.[225] False positive differentials can be particularly important for 1:N systems, because growth in gallery size increases the false positive rate (intuitively because there are more potential matches for every search).

The research literature has less to say about non-algorithmic sources of demographic differentials, because these depend more on the details of specific use cases.[226] These factors are best addressed through operational testing of a particular system.

[220] *Id.* at 7.

[221] *See*, *e.g.,* Gabriella Pangelinan et al., *Exploring Causes of Demographic Variations in Face Recognition Accuracy*, (Apr. 14, 2023), https://arxiv.org/pdf/2304.07175v1; Seyma Yucer et al., *Racial Bias within Face Recognition: A Survey,* ACM Computing Surveys 57, 4, Art. 105 (Dec. 23, 2024). https://doi.org/10.1145/3705295 [hereinafter Yucer].

[222] *Face Recognition Technology Evaluation (FRTE) 1:1 Verification*, *supra*.

[223] Patrick Grother, *Face Recognition Vendor Test (FRVT) Part 8: Summarizing Demographic Differentials, NISTIR 8429,* NAT'L INST. OF STANDARDS AND TECH (July 2022), at i, https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8429.ipd.pdf.

[224] *Face Recognition Technology Evaluation (FRTE) 1:1 Verification*, *supra*.

[225] *Face Recognition Vendor Test (FRVT) Part 8: Summarizing Demographic Differentials, supra,* at i.

[226] *But see* Yucer, *supra.*

C. Demographic Differential Performance of FRT Algorithms Used by TSA

IDEMIA's 1:1 algorithm submitted to NIST on August 6, 2024 (idemia-011) showed a difference of 5.36 times between the demographic group with the lowest false positive rate (Central American males aged 12–20) and the group with the highest false positive rate (West African women aged 65 and older). Although this differential appears large, the absolute rates were still fairly small (0.022% and 0.118% respectively) and also represented the lowest magnitude differential observed by NIST.[227] Considering the maximum false positive rate to an average across all demographic groups, idemia-011 scored the best (that is, had the lowest differential) of all 586 entries considered.

For false negatives, IDEMIA's most recent algorithm showed a differential of 1.09 times between the group with the highest rate (West African individuals at 0.21%) and the average across demographic groups.[228] In other words, West African individuals could experience false negative results 9% more frequently than the average of the overall population. This is the 158th lowest differential of 586 tested in NIST's testing. Note, however, that many algorithms with lower relative differentials also had higher overall rates of false negatives.

As previously discussed in Section II.B, in February 2024, DHS S&T and TSA released an evaluation of scenario testing considering demographic performance for CAT-2 based on self-reported demographic attributes, including age, gender, race, and ethnicity, as well as measured skin tone, of over 1,600 volunteer participants.[229] Because the test was statistical in nature, it would not have been able to detect with statistical confidence any differences smaller than a margin of error (which varied across different comparisons). The test aimed to detect absolute demographic differentials of 5% or greater, and the volunteer demographic information was then used to determine performance metrics. Overall, the system correctly matched 99.4% of participants, and 99.9% of those participants for whom the system successfully acquired both a live image and the image from their presented identification document. The study did not detect statistically significant differences in performance of the core face comparison algorithm by gender, race, or ethnicity under varied test conditions. However, it did detect differences due to other operational factors: older adults showed a small but statistically significant differential in the rate of failure to

[227] *Face Recognition Technology Evaluation (FRTE) 1:1 Verification*, *supra.* Differential measured as the higher rate divided by the lower rate; that is, the false positive rate for West African women 65 and older is 24 times higher than the false positive rate for Central American males 50–65. No other algorithm showed a difference smaller than that between the lowest and highest false positive rates for particular demographic groups. *Id.*

[228] *Id.* NIST's demographic differential performance summary does not include the impact of gender.

[229] DHS S&T 2024 Demographic Study, *supra*.

acquire images (1.0% for above 60 compared to 0.0% for those 45 and under). Testing also showed a statistically significant differential in the rates for which the identification documents were rejected based on race (2.4% for Black participants compared to 0.5% for White participants). TSA and DHS S&T have not yet identified the source of this differential failure mode; however, it does not result from the performance of the FRT software or algorithm.

As also discussed in Section II.B, DHS S&T and TSA most recently tested the 1:N technology in the fall of 2024 using both scenario testing and operational data. On average, the face capture technology worked 93% of the time; this lower performance was found to be caused by an issue with the face detection algorithm, which led to variations in face capture performance based on age, gender, race, and skin tone.[230] In response to these findings, TSA introduced a feature to allow the TSO to manually override the face detection algorithm when it does not work.[231] Based on testing in December 2024, this adds 2–3 seconds to the process. TSA and DHS S&T are evaluating new algorithms to improve this step and plan to test and implement them later in 2025.[232]

DHS also measured the transaction time, or “efficiency.” The efficiency was eight seconds on average. All demographic groups were within one second of the average, and it took less than nine seconds for all demographic groups.

DHS S&T and the Maryland Test Facility (a lab affiliated with DHS established to support the testing of biometric and non-biometric technologies) plan to conduct a small-scale experiment in summer 2025 with participants “to interact with the 1:N technology unit to test each face capture algorithm. They will use the results to determine the best face capture algorithm for TSA’s use case and then conduct a larger, lab-based test” to ensure that TSA systems satisfy the requirements set forth in DHS Directive 026-11 for a demographically diverse population.[233]

[230] In testing, face capture worked 89% of the time for those aged 61+ years. It worked 94–96% of the time for those under age 61 years, showing a difference in performance based on age. Face capture worked 91% of the time for male volunteers, compared to 95% for female volunteers, showing a difference in performance based on gender. Face capture worked 88% of the time for those with darker skin tones, compared to 94–97% of the time for those with lighter skin tones. This shows a difference in performance based on skin tone. Additionally, it worked 91% for participants who identified as Black or African American, compared to 96% for those who identified as white. *Implementation of DHS Directive 026-11, supra,* at 41.

[231] *Id.*

[232] *Id.*

[233] *Id.* at 42.

The results of these tests make it possible for TSA to investigate and seek to mitigate detected differentials. Future operational tests could evaluate the success of any mitigation efforts and detect any new differentials that might emerge due to evolution of the CAT system and its uses.

D. Conclusion

Errors in the operations of FRT can affect system efficacy as well as burden individuals. More specifically, false positives are more likely to reflect security issues, such as failing to detect impostors (and thus letting them proceed through the security checkpoint) or mistakenly identifying one legitimate traveler for another, but they are less likely to inconvenience travelers; false negatives may burden travelers and TSOs. These failure rates are linked by how the operators set the threshold.

Demographic differential performance of FRT systems has been repeatedly confirmed by independent testing and evaluation from the private sector, academic researchers, and government testing labs. Rate disparities from false negatives mean, for example, that the burden of additional scrutiny arising from a failure of the FRT system to recognize individuals may fall disproportionately on some groups, including older individuals and those who have been historically disadvantaged and marginalized.[234] However, current testing has not measured the impact of the CAT-2 systems in the field across different demographic groups to understand whether and how particular groups are affected.

The absolute magnitude of the differences has decreased along with overall improvement in the performance of algorithms, but has not disappeared, and although DHS S&T testing did not detect statistically significant differentials in performance of the core face comparison algorithm across demographic subgroups in the CAT-2 system, NIST testing continues to show that relative differentials in the algorithms, while small, have persisted.

[234] *See* NAS FR Report, *supra*, at 3.

IV. TRANSPARENCY AND PUBLIC NOTICE

Transparency regarding a program's operations and policies is a prerequisite for informed debate and policy analysis. This encompasses approaches such as providing sufficiently detailed descriptions of how the program works; public notice regarding the purposes and practices for the collection, use, and retention of PII; and disclosure of risks generated by the program and efforts to mitigate those risks.

Transparency about a technology like FRT, or any technology that generates substantial public concern, is critical: meaningful transparency advances public awareness of and trust in such technology. In addition to meeting policy and statutory requirements, transparency enables and bolsters public trust. It also enables informed debates and policy analyses. A detailed description of how a technology or program works must include: a) rules about PII collection, use, dissemination, and retention; b) an assessment of potential privacy and civil liberties risks generated by the deployment of the technology; and c) public disclosure of those assessments and the steps planned to mitigate any risks.

A. Public Disclosures

TSA has released multiple publicly available resources to inform the public about its use of FRT in airports and to provide details of the programs as they have been in development. TSA has also worked with Congress to provide information and transparency about TSA's use of FRT. As described above, TSA released its Biometrics Roadmap in 2018 laying out options and plans for future deployment of the technology. CBP and TSA delivered a report to Congress in 2019 about their use of and plans for biometric technologies.[235] The report included an overview of CBP's and TSA's strategies and plans for using facial recognition in airports, a description of perceived operational and security benefits, an assessment of potential privacy risks and mitigations, and a discussion of CBP and TSA analyses and assessments of performance issues.

[235] U.S. Dep't of Homeland Sec., *Report to Congress, Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies* (Aug. 2019).

TSA regularly releases press releases and statements when FRT pilots expand to more airports,[236] and local and national news outlets frequently publish articles that reference TSA information.[237] TSA describes the use of facial recognition on its website, including a "fact sheet" that describes the technology[238] and provides answers to frequently asked questions.[239]

As required by the E-Government Act of 2002,[240] TSA has published five versions of a PIA regarding its testing of facial recognition for identification at the TDC between January 2018 and November 2023.[241] Each PIA discloses aspects of the pilot testing at the time of publication, including expansions to particular airports, integration with other TSA programs such as Secure Flight, and testing of different modes of recognition (i.e., 1:1 vs. 1:N). The evolution of the program over time has meant that earlier descriptions contained in PIAs or observed by participants have not always been accurate at later stages. For instance, in the early development of the pilot, TSOs could not turn off the camera on the CAT device.[242] At the time, the only way to allow travelers to opt out of having their picture taken was to go to a different lane for manual processing.[243] TSA has since begun using more recent

[236] *See, e.g.,* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *New credential authentication technology units installed at Albany and Syracuse Hancock International Airports ahead of the busy Thanksgiving holiday travel period* (Nov. 17, 2023), https://www.tsa.gov/news/press/releases/2023/11/17/new-credential-authentication-technology-units-installed-albany-and.

[237] *See, e.g.,* Christine Chung, *Facial Recognition: Coming Soon to an Airport Near You*, N.Y. TIMES (Feb. 18, 2024), https://www.nytimes.com/2024/02/18/travel/facial-recognition-airports-biometrics.html.

[238] U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Facial Recognition Technology*, https://www.tsa.gov/news/press/factsheets/facial-recognition-technology (last visited Apr. 15, 2025).

[239] U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Biometrics Technology*, https://www.tsa.gov/biometrics-technology (last visited Apr. 15, 2025).

[240] The E-Government Act of 2002 requires all federal agencies to conduct PIAs when "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form;" or when an agency "initiat[es] a new collection of information that . . . will be collected, maintained, or disseminated using information technology . . . and includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government." Pub. L. 107-347, § 208, 116 Stat. 2921–2922 (2002). The Act requires an agency to make PIAs publicly available, except when an agency determines that publication of the PIA would raise security concerns or would reveal classified, sensitive, or private information. *Id.*

[241] *See* U.S. Dep't of Homeland Sec., *TSA Travel Document Checker Privacy Impact Assessments*, https://www.dhs.gov/publication/dhstsapia-046-travel-document-checker-automation-using-facial-recognition (last visited Apr. 15, 2025).

[242] PCLOB Phone Call with TSA and DHS (Feb. 9, 2024).

[243] *Id.*

prototypes of the CAT device that include a toggle switch that allows TSOs to manually turn the CAT camera on and off.[244]

TSA informational websites direct the public to reference the FRT PIAs if they wish to learn more about the pilots and associated privacy mitigations, but a member of the public would not easily be able to refer to the PIAs and understand which one describes the current phase of the technology. TSA's use of FRT has expanded dramatically since 2018, when the first PIA discussing the use of FRT at the TDC was published. Since then, TSA's pilots have evolved from using biometric-enabled automated security gates to implementing integrated facial recognition at the CAT device, and finally to the Secure Flight connection and the 1:N pilot. As of April 2025, TSA has not yet produced a comprehensive PIA describing the system, despite the program reaching initial operational capability in March 2024. TSA has stated that it has begun drafting a comprehensive PIA to describe the system and anticipates that it will be completed by the end of 2025.

B. Program Terminology

TSA has referred to its use of FRT in airports as a "proof of concept" or "pilot" from the program's inception in 2017 through at least 2024. TSA's early tests using FRT, which employed prototype equipment deployed at a single lane of an airport for several weeks, could reasonably be considered "proofs of concept" or "pilot tests." However, even before TSA officially acknowledged that aspects of the program had reached initial operational capability in 2023, the program had been deployed at multiple checkpoint lanes at dozens of the busiest airports in the United States. Although TSA did not provide numbers of travelers that passed through checkpoints using CAT-2 machines, the number is likely in the millions. This level of operational deployment is broader than what would traditionally be considered a "proof of concept" or "pilot." TSA's continued description of the program as a "pilot" suggested that it was limited in scope and impact, and that TSA was still in the process of evaluating it as a potential option. However, at least as early as 2023, TSA had committed to a nationwide deployment of FRT systems.

C. Algorithmic Transparency

Traditionally, the public has had limited access to information about commercial software used by the government. This practice has been maintained for multiple reasons. Among others, commercial vendors have an interest in protecting their proprietary information and the government has an interest in maintaining operational security. However, disclosure of some degree of technical details of the operation of FRT systems is

[244] *Id.*

warranted to evaluate whether the government is employing algorithms with sufficient accuracy and acceptably minimal demographic differential performance.

TSA CAT-2, like other FRT systems (and indeed many AI systems), embeds proprietary commercial algorithms to generate templates from images and to calculate a similarity score when comparing two templates. The contents and nature of the data set, such as the demographics of the people pictured, can affect the ways in which the algorithm functions.

The ability to evaluate ML-trained AI systems begins with public transparency around the data sets used for training. There are multiple proposals for establishing standards and best practices around documenting data sets, such as providing information about attributes like the data set's provenance, representation, usage, and evaluations relating to fairness. These include "Data Cards,"[245] "Data Nutrition Labels,"[246] and "Datasheets for Datasets."[247]

As described above, NIST performs extensive testing of facial recognition algorithms and makes the results of those tests public. NIST's testing and related reports substantially contribute to the public's understanding of the capabilities and limitations of FRT technology broadly and of specific vendors. However, algorithms submitted for NIST testing are identified in NIST disclosures only by vendor name plus a sequential number and are not associated with particular public release identifiers of the software such as a version number.[248] TSA has clearly communicated in PIAs and other public reporting that the CAT-2 1:1 matching algorithm is developed by IDEMIA. Similarly, CBP has disclosed that NEC Corporation developed the algorithm used in TVS, which TSA uses for 1:N recognition. However, in both cases, the public does not have access to information that explains which versions submitted to NIST correspond to the particular versions of those algorithms used by TSA or CBP.

D. Conclusion

TSA has made a serious but incomplete attempt to be transparent and inform the public about the CAT-2 FRT capabilities. The materials describing aspects of the program were accurate at the time of publication and include relevant information. However, as the program changed and evolved, it was not always clear whether previous PIAs continued to describe the program or its practices accurately. By focusing PIAs on individual iterations of

[245] *See* Mahima Pushkarna et al., *Data Cards: Purposeful and Transparent Dataset Documentation for Responsible AI*, ASSOC. FOR COMPUTING MACHINERY, CONF. ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY, at 1776–1826 (2022), https://doi.org/10.1145/3531146.3533231.

[246] The Data Nutrition Project, *Mission*, https://datanutrition.org/ (last visited Apr. 15, 2025).

[247] *See* Timnit Gebru et al., *Datasheets for Datasets* (Dec. 2021), https://arxiv.org/pdf/1803.09010.pdf.

[248] For example, idemia_010 is the tenth algorithm submitted to NIST by IDEMIA.

the pilot tests, and not publishing a single, comprehensive PIA that describes the program as it is intended to operate after the conclusion of the pilot, TSA allowed for potential confusion about the maturity and scope of the program. As of April 2025, TSA has not published a comprehensive PIA on the operational CAT-2 FRT capabilities. TSA plans to publish a comprehensive PIA on the FRT system by the end of 2025.

While TSA has attempted to inform the public about expansion of FRT use and general features of updated technology, there has been a lack of clear communication about the nature of FRT deployment. Terms like “pilot,” “proof of concept,” and “operational deployment” have been used inconsistently and can also be misleading when compared to the reality of how the technology is being used at airports.

While TSA has attempted to inform the public about expansion of FRT use and general features of updated technology, there has been a lack of clear communication about the nature of FRT deployment.

Transparency regarding algorithms is inherently more complex for an agency to implement, as details about algorithm accuracy and testing are typically technical in nature and difficult to communicate to non-technical audiences in a meaningful way. Algorithms are also updated regularly and the relationship between algorithm version, available test results, and the actual technology a traveler may encounter at the airport is not always clear. TSA has taken a good first step in regularly conveying what company develops its algorithm, but to keep the public informed and allow informed participation, TSA and S&T should work together to explore ways to provide succinct and clear public notice that is broadly accessible to non-technical audiences about what algorithms are in use and their relevant test results, in ways consistent with national security.

V. INDIVIDUAL RIGHTS AND NOTICE

Millions of travelers fly through U.S. airports every day, bringing many people into contact with TSA's FRT system. These interactions occur at a known time and place, creating both a responsibility and an opportunity to disclose the program's operation, a description of the program, and individuals' rights surrounding participating in the program, such as the ability to opt out.

The previous section discussed ways in which TSA informs the general public about the operations of the program, its risks and controls, and the ways in which it may use personal information. This section discusses the rights that individuals have when interacting with TSA FRT systems, how TSA informs individuals of those rights, the extent to which the provided safeguards are sufficient to protect the privacy and civil liberties of participants, and the ability of individuals to seek redress when they feel that their rights have been infringed.

A. Voluntary Participation (Opting In and Opting Out)

The voluntary nature of participation in the TSA FRT systems discussed in this report is governed by departmental policy. When DHS uses FRT for verification in a non-law enforcement related context, it is required to afford U.S. citizens the right to opt out and provide an alternative method of processing, and is required to provide alternative processing to resolve match or no match outcomes.[249] The process of opting out and completing alternative processing "may not impose additional burdens or requirements on the individual beyond what is necessary to complete the verification process."[250]

Presently, for the 1:1 matching system, travelers may choose to opt out of FRT matching when they reach the TDC station at security checkpoints.[251] The limited evidence available suggests that opting out is rare: in TSA testing in the summer of 2019, during which signage and TSA agents informed travelers that they could opt out of the test, 0.18% of approximately 13,000 travelers involved in the FRT pilot chose to do so.[252]

[249] DHS Directive 026-11, *supra*, at 6. However, as discussed above, the status of DHS Directive 026-11 is unclear.

[250] *Id*.

[251] U.S. Dep't of Homeland Sec., Customs and Border Prot., *Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States, Notice of Proposed Rulemaking* (Nov. 19, 2020), https://www.federalregister.gov/documents/2020/11/19/2020-24707/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states.

[252] *Id.*

TSA policies and procedures for operating CAT-2 devices define how TSOs respond when travelers request to opt out of 1:1 recognition. If a traveler does so, the TSO will turn the camera off to avoid the system taking a photo. The TSO will still use the CAT-2 device to authenticate the traveler's identification document and determine that the traveler has a valid boarding pass for that day. The TSO then manually compares the image on the traveler's identification document to the traveler's appearance, rather than using the FRT software in the CAT-2 system to determine a match. According to TSA procedures, travelers who opt out should not be required to wait in a longer or separate line. However, complaints submitted to TSA's Contact Center (TCC) suggest that TSOs may not be uniformly implementing this opt-out policy.[253]

For the 1:N system, eligible travelers are offered the choice to opt in to the program. To be eligible, travelers must be enrolled in a Trusted Traveler Program such as TSA PreCheck, be a member of a participating airline's frequent flyer program, and be using the airline's mobile application. Those eligible will be informed that they can opt into FRT if they are traveling from an airport using the technology. They may later choose to opt out.

Beyond current policy and practices, former TSA Administrator David Pekoske publicly suggested that biometric assessment will eventually be required for all travelers.[254] However, adopting such mandatory use of biometrics for non-law enforcement purposes would require changes to, or repeal of, DHS Directive 026-11. TSA states that it currently has no plans to mandate the use of FRT at airport checkpoints for identity verification purposes.

B. Individual Notice

TSA policy requires that signage be posted at all checkpoint lanes to disclose that travelers may be identified using facial recognition, that photographs will be deleted after matching, and that travelers have the right to decline participation.[255] As described in more detail below in Section VI.D., TSA periodically collects data from CAT devices for performance assessment testing.[256] During these periods, the agency posts additional

[253] TSA Responses to Fourth Round of PCLOB Questions, Copy of Complaints (Feb. 2024).

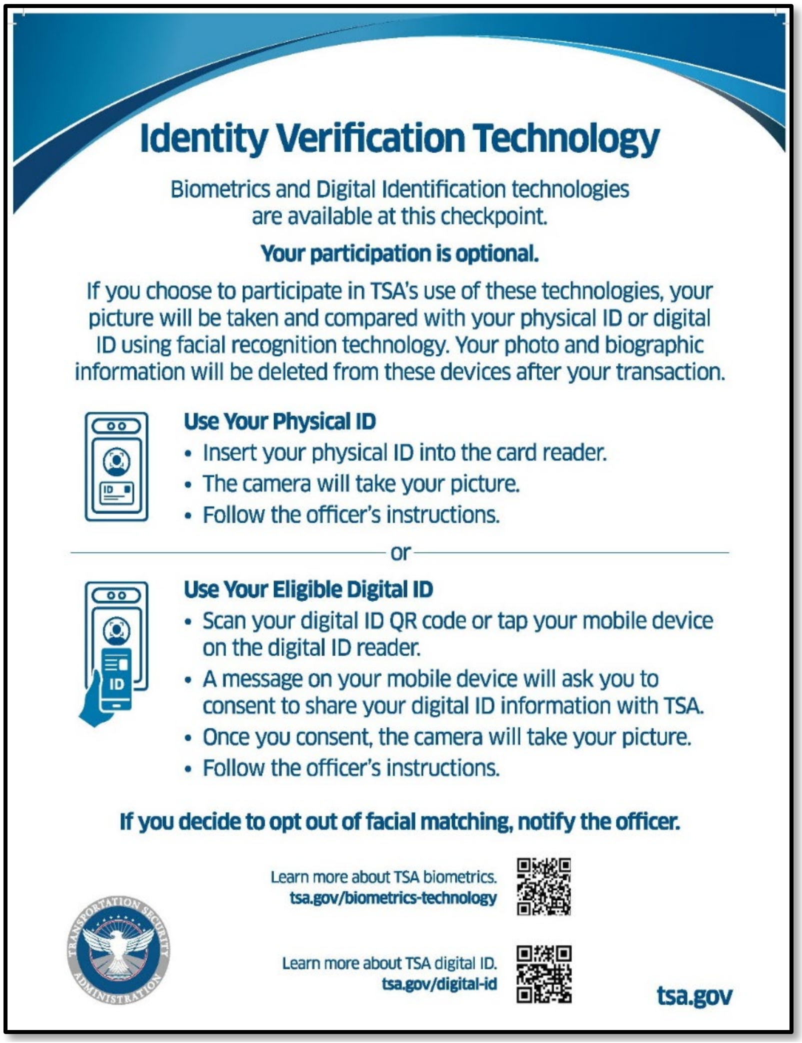
[254] *Accelerating Aviation Security: Innovative New Technology Keeping The Skies Safe*, *supra*, at 08:22–08:31.

[255] U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Checkpoint Requirements and Planning Guide (CRPG): August 2024 Edition,* at 4-2–4-3 (Sept. 12, 2024). TSA's guidance document on airport signage and checkpoint requirements has been removed from the DHS website; however, an archived web version of this report can be found at: https://web.archive.org/web/20250321031318/https://www.tsa.gov/sites/default/files/checkpoint-requirements-and-planning-guide.pdf.

[256] *See DHS/TSA/PIA-046(d) Travel Document Checker Automation Using Facial Identification*, *supra*, at 5.

signage near the testing lanes and makes handouts available describing this additional data collection. The 1:N program uses a notice and opt-in system described below.

TSA has updated the signage associated with the FRT systems multiple times since at least 2023. Iterations have involved using "clear language that notifies travelers they may decline having their photo taken;"[257] highlighting the optional nature of participation for 1:1 and 1:N programs; and adding that travelers' photographs are deleted after verification, that travelers can inform the TSO if they wish to opt out, and that they will not lose their place in line if they opt out.[258] TSA has stated that it is committed to continually evaluating and improving public messaging and notice.



Identity Verification Technology

Biometrics and Digital Identification technologies are available at this checkpoint.

Your participation is optional.

If you choose to participate in TSA's use of these technologies, your picture will be taken and compared with your physical ID or digital ID using facial recognition technology. Your photo and biographic information will be deleted from these devices after your transaction.

Use Your Physical ID

- Insert your physical ID into the card reader.
- The camera will take your picture.
- Follow the officer's instructions.

or

Use Your Eligible Digital ID

- Scan your digital ID QR code or tap your mobile device on the digital ID reader.
- A message on your mobile device will ask you to consent to share your digital ID information with TSA.
- Once you consent, the camera will take your picture.
- Follow the officer's instructions.

If you decide to opt out of facial matching, notify the officer.

Learn more about TSA biometrics.
tsa.gov/biometrics-technology

Learn more about TSA digital ID.
tsa.gov/digital-id

tsa.gov

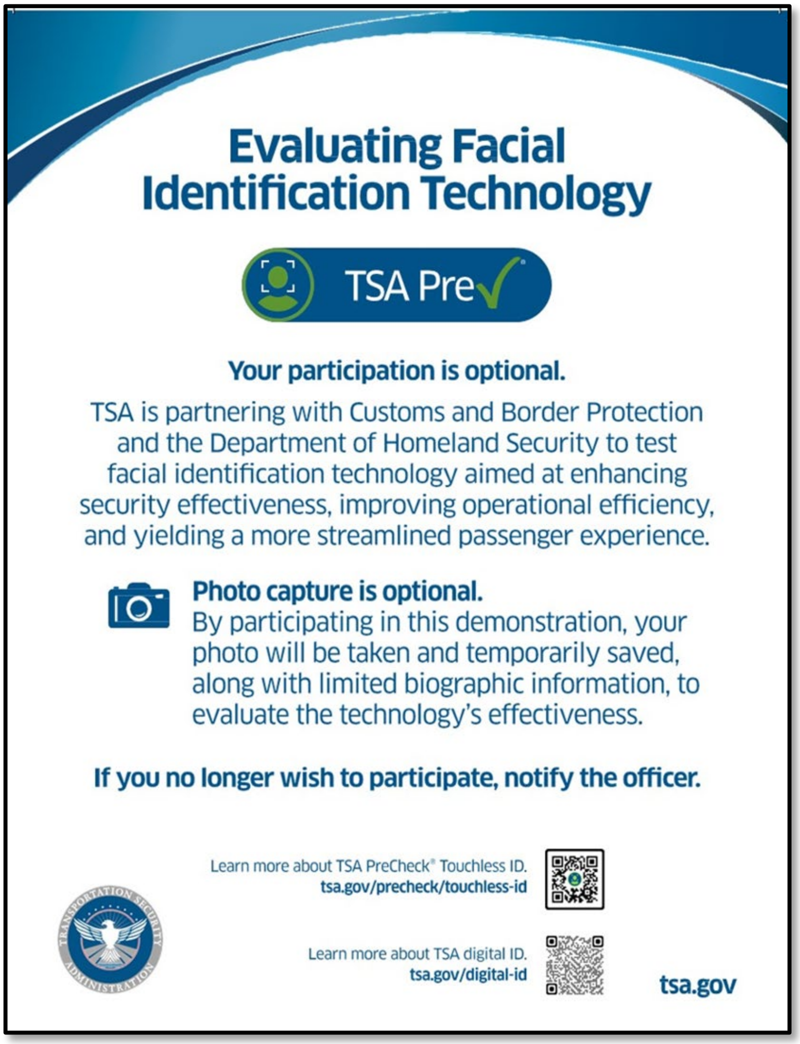
Above: TSA signage for 1:1 FRT placed at TSA security checkpoints. Image provided by TSA.

Both because of the changing nature of TSA's signage over time as well as the scope of the nationwide deployment, PCLOB did not undertake a comprehensive review of signage across airports to determine sufficiency or efficacy. However, as we discuss in Part 3, we recommend that TSA perform regular assessments of such issues.

[257] Edward Graham, *TSA uses 'minimum' data to fine-tune its facial recognition, but some experts still worry*, NEXTGOV/FCW (Jan. 29, 2024), https://www.nextgov.com/emerging-tech/2024/01/tsa-uses-minimum-data-fine-tune-its-facial-recognition-some-experts-still-worry/393672/.

[258] U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Facial Recognition Technology*, https://www.tsa.gov/news/press/factsheets/facial-recognition-technology (last visited Apr. 16, 2025).

Below: TSA signage for 1:N FRT (TSA PreCheck Touchless ID) currently placed at TSA security checkpoints in 10 participating airports. Image provided by TSA.



Evaluating Facial Identification Technology

TSA Pre✓

Your participation is optional.

TSA is partnering with Customs and Border Protection and the Department of Homeland Security to test facial identification technology aimed at enhancing security effectiveness, improving operational efficiency, and yielding a more streamlined passenger experience.

Photo capture is optional.
By participating in this demonstration, your photo will be taken and temporarily saved, along with limited biographic information, to evaluate the technology's effectiveness.

If you no longer wish to participate, notify the officer.

Learn more about TSA PreCheck® Touchless ID.
tsa.gov/precheck/touchless-id

Learn more about TSA digital ID.
tsa.gov/digital-id

tsa.gov

For the 1:N program, travelers are informed of the program when they check in for their flight and are given a choice to opt in and consent to TSA's use of their PII. Their boarding passes are then marked with a consent marker. Individuals whose boarding passes do not contain this marker are not eligible to participate.[259] Participating airlines provide travelers with information about the program and inform them that they can choose not to participate at any point once they arrive at the airport.

Advocacy groups and members of Congress have stated concerns about the sufficiency of TSA's notice and transparency.[260] Such concerns include that unclear or inadequate signage could lead to individuals being unaware that TSA is using facial

[259] *See DHS/TSA/PIA-046(d) Travel Document Checker Automation Using Facial Identification*, *supra*, at 3.

[260] In a press release describing their proposed Traveler Privacy Protection Act in November 2023, Senators Kennedy and Merkley stated that "despite the TSA calling its plan to implement facial scans at more than 430 U.S. airports voluntary, passengers are largely unaware of their ability to opt out. Moreover, TSA does not effectively display notices at its check points to inform travelers that they have such an option." Sen. John Kennedy, *Kennedy, Merkley introduce bill to end involuntary facial recognition screenings, protect Americans' privacy* (Nov. 29, 2023), https://www.kennedy.senate.gov/public/2023/11/kennedy-merkley-introduce-bill-to-end-involuntary-facial-recognition-screenings-protect-americans-privacy; *see also Sen.* Jeff Merkley, *Merkley and the Challenge of Facial Recognition Technology* (July 18, 2023), https://www.merkley.senate.gov/merkley-and-the-challenge-of-facial-recognition-technology/2024.

recognition, uninformed about how TSA is using this technology or their personal information, or unaware that they have the option to decline participation by opting out.

In 2020, the GAO reported on DHS's use of FRT in airports and its incorporation of privacy protection principles into those systems. Though GAO stated that it was too early to conduct a full assessment, it found that TSA's facial recognition pilot tests have incorporated privacy protections consistent with the Fair Information Practice Principles (FIPPs),[261] such as transparency, consent, and redress.[262]

As described in more detail in Section VI.D. below, TSA periodically collects data from CAT devices for performance assessment testing.[263] During these times, the agency posts signage near the testing lanes and "make[s] handouts available that provide additional information about TSA's screening technology and data protection procedures."[264] The CAT program office assesses signage and associated procedures during the testing process and works with the TSA Requirements and Capabilities Analysis office to evaluate the effectiveness of those procedures based on feedback from the field and operational requirements.[265]

C. Redress

TSA and DHS offer opportunities for travelers to submit complaints or requests for compensation for situations in which they believe that they have been harmed by actions of TSA while traveling.[266] We refer to the procedures for receiving, investigating, and

[261] The Homeland Security Act of 2002, as amended, requires the DHS Chief Privacy Officer to "assur[e] that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974." Homeland Security Act of 2002, 6 U.S.C. § 142; *see* Privacy Act of 1974, as amended, 5 U.S.C. § 552a. Further, DHS policy requires that the department consider the Fair Information Practice Principles (FIPPs), a set of widely accepted privacy principles that are at the core of the Privacy Act of 1974, whenever a DHS program or activity involves the collection of PII or raises concerns about privacy. *DHS Privacy Policy Guidance Memorandum 2008-01, supra,* at 3.

[262] U.S. Gov't Accountability Office, *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues, GAO-20-568*, at 66–67 (Sept. 2020), https://www.gao.gov/assets/gao-20-568.pdf.

[263] *See DHS/TSA/PIA-046(d) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification, supra*, at 5.

[264] *TSA uses 'minimum' data to fine-tune its facial recognition, but some experts still worry*, *supra*. TSA states that such handouts are available "upon request" from a traveler. TSA Response to PCLOB Request (Apr. 17, 2025).

[265] TSA Responses to Fourth Round of PCLOB Questions, Q. 15(a) (Feb. 2024).

[266] These complaints could include discrimination, broken locks on luggage, unprofessional behavior by TSA employees, or others. *See* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *DHS Traveler Redress Inquiry Program*, https://www.tsa.gov/travel/security-screening/travel-redress-program (last visited Apr. 16,

responding to these complaints broadly as "Redress." Travelers seeking redress can use the DHS Traveler Redress Inquiry Program[267] (TRIP) or the TCC.[268] The TCC is part of TSA's Civil Rights and Liberties, Ombudsman, and Traveler Engagement Office and provides a contact phone number as well as web forms for submitting claims relating to damage during screening,[269] violations of civil rights,[270] and other complaints.[271] Individuals may also submit claims relating to discrimination to DHS CRCL.[272]

The forms available on the TRIP and TCC websites require the user to indicate the category of their complaint.[273] Neither form offers a choice that corresponds to concerns or complaints specifically regarding the use of facial recognition or biometric matching and identification. Instead, travelers wishing to submit such a claim must pick some other choice such as "civil rights" or "screening," even if these are not apt. Despite these limitations, TSA identified at least 97 complaints that referenced the use of FRT from May 2023 through February 2024.[274] The complaints included TSA personnel providing inaccurate information about the ability to opt out, signage not being present, and general lack of information about the nature of the pilot and what information about the traveler is collected and retained.

2025); U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Complaint Form,* https://www.tsa.gov/contact-center/form/complaints (last visited Apr. 16, 2025).

[267] The DHS TRIP website has two separate redress application processes: DHS TSA TRIP handles traveler inquiries related to domestic travel, and DHS CBP TRIP is for international travelers. *See* U.S. Dep't of Homeland Sec., *Traveler Redress Inquiry Program*, https://trip.dhs.gov/ (last visited Apr. 16, 2025).

[268] U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Customer Service*, https://www.tsa.gov/contact/customer-service (last visited Apr. 16, 2025).

[269] U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Claims*, https://www.tsa.gov/travel/security-screening/claims (last visited Apr. 16, 2025).

[270] U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *TSA Cares, Civil Rights*, https://www.tsa.gov/travel/tsa-cares/civil-rights (last visited Apr. 16, 2025).

[271] U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Complaint Form,* https://www.tsa.gov/contact-center/form/complaints (last visited Apr. 16, 2025).

[272] U.S. Dep't of Homeland Sec., Off. for C.R. and C.L., *CRCL Complaints*, https://engage.dhs.gov/crcl-complaint?id=crcl_intake&sys_id=154d32711b4c9110b930628ae54bcb4f&lang=english (last visited Apr. 15, 2025). Of course, DHS must maintain adequate staffing to ensure such complaints are adjudicated effectively.

[273] For TRIP, these categories are "unable to print a boarding pass," "denied boarding," "denied entry to or exit from the U.S.," and "continually referred for additional screening." *See* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *DHS Traveler Redress Inquiry Program*, https://www.tsa.gov/travel/security-screening/travel-redress-program (last visited Apr. 16, 2025). For TCC, these categories are "broken locks," "civil rights and liberties," "lost and found," "missing or damaged items," "prohibited items," "professionalism and customer service," "screening," and "TSA PreCheck." *See* U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Complaint Form,* https://www.tsa.gov/contact-center/form/complaints (last visited Apr. 16, 2025).

[274] TSA Responses to Fourth Round of PCLOB Questions (Feb. 2024). TSA indicated that it receives approximately 2,000 complaints overall per day.

Further, neither TCC nor TRIP have specific procedures corresponding to such biometric-related complaints. For example, for a traveler who submits a complaint that the system repeatedly fails to recognize them, there are no defined procedures for investigating whether the claim is accurate or offering potential solutions. Such investigation may require additional data collection and retention beyond what is currently performed and thus may require additional mitigation and protection.

The ability to collect and respond to feedback accurately and efficiently is key for any system, and especially those that are still being developed or evaluated. First, for some situations, it may be possible to respond to the individual with useful guidance. For example, repeated matching failures might be caused by a poor-quality driver's license photo. A potential redress procedure in this instance could suggest that possibility, provide links to tools for image quality evaluation, and direct travelers to the appropriate office at their state's DMV. Second, such complaints may serve as a means to measure the effectiveness of the program. For example, repeated complaints that travelers were unaware of the ability to opt out or that TSA employees refused requests to opt out would suggest that there are gaps in TSA's signage, training, and public notice. Similarly, complaints from individuals of particular demographic groups that the system repeatedly fails to recognize them could suggest potential problems in the system's matching accuracy. Clusters of similar complaints taking place in particular airports or checkpoints, or patterns of similar complaints across sites, should prompt TSA to investigate whether there are factors contributing to performance issues at those locations or functions and to take steps to address any such issues.

D. Conclusion

The 1:1 facial recognition program should remain voluntary for all passengers. Travelers should retain the ability to opt out of 1:1 facial recognition without penalty or additional burdens, such as being required to wait in a longer or separate line.

Voluntary participation ensures travelers can exercise meaningful consent in determining whether to participate in the FRT programs. Consistent with DHS policy on FRT, the 1:1 facial recognition program should remain voluntary for all passengers. Travelers should retain the ability to opt out of 1:1 facial recognition without penalty or additional burdens, such as being required to wait in a longer or separate line. A further decision to make the program mandatory or expand the 1:N program, such as by changing it to an opt-out program or changing the composition or construction of the gallery, would require a reassessment of the balance presently being struck between national security and privacy and civil liberties. Similarly, changes in the nature of the threat or effectiveness of the program could suggest the need for a reassessment of the program's comparative risks and benefits.

While TSA policy requires that signage and TSO instruction make clear to travelers the voluntary nature of participation, there is evidence that these policies have historically not been implemented consistently. There are undeniable difficulties in establishing a program that is frequently evolving, including logistical challenges related to screening lanes and auditing performance, but travelers must be informed that they can opt out and given a meaningful opportunity to do so.

DHS and TSA do not have defined procedures for receiving, assessing, and investigating complaints specific to the operation of FRT systems. The lack of such procedures means that not only are they not aware of the extent to which FRT is causing issues for travelers, but they do not have the opportunity to investigate and resolve such issues.

VI. Collection, Sharing, Retention, and Use of Data

This section describes and evaluates TSA's collection, use, and retention of biographic, biometric, and biometric-derived data in its FRT systems. TSA's use of FRT involves multiple systems that interact with traveler information. In both the 1:1 and 1:N systems, information is collected, transmitted, and used by TSA's Secure Flight, the TSA CAT-2 device, and DHS S&T. With 1:N identification, information is also received from and sent to CBP's TVS. Data retention and sharing policies for the TSA FRT system differ between normal operations and a special data-collection mode used for system evaluation, described in more detail below.

As a general matter, the more information gathered, the more places it is stored, and the longer it is retained, the higher the chance that the information could be accessed by malicious actors or misused beyond its intended purpose. The following section discusses certain information security safeguards that TSA has adopted.

A. Data Collection

Prior to the traveler arriving at the security checkpoint, Secure Flight collects from airline reservation systems information identifying the traveler (such as name, sex, and passport number) and information about their travel (such as itinerary number, passenger record locator, and reservation status). Traveler identification information is compared with entries on the Terrorist Watchlist[275] to identify individuals on the No Fly List or those who will require enhanced or secondary screening. TSA systems transmit this traveler information to the appropriate airport. At the checkpoint, the CAT-2 device uses this information to confirm that the traveler arriving at the checkpoint has a valid reservation on that day at that airport and as a basis of comparison between the traveler and the identity document the traveler presents (when using 1:1 identity verification).

The CAT-2 device takes a photograph of travelers who have not opted out of the 1:1 system or have opted into the 1:N system. For all travelers using checkpoints employing 1:1 identity verification, including those travelers who opt out of biometric comparison, the CAT-2 device collects information from the identity document presented by the traveler, such as name, date of birth, identification type, and certain document-specific fields such as passport number. This information is compared with Secure Flight Passenger Data for that traveler.

[275] For more information on the Watchlist, *see* Fed. Bureau of Investigation, *Terrorist Screening Center*, https://www.fbi.gov/investigate/terrorism (last visited Apr. 16, 2025); *see generally* U.S. Priv. and C.L. Oversight Bd., *Report on the Terrorist Watchlist, supra.*

When using 1:N identification, the traveler does not present an identity document to the CAT-2 device or TSO, and so that information is not collected.

B. Information Sharing and Dissemination

Other than as described below for evaluation purposes, TSA does not further share or distribute any information gathered by the CAT-2 device during 1:1 operations.

For the 1:N system, TSA shares biographic information from Secure Flight, including passport information, Known Traveler Number, name, sex, date of birth, and departure airport/time with CBP TVS in order for TVS to assemble the appropriate gallery of images.[276] TSA also transmits a live photo to CBP TVS to perform the comparison and attempt to identify a match with an image in the gallery. TVS then transmits back to the CAT-2 the biographic information corresponding to the match identified from the gallery, along with metadata regarding the transaction.

Secure Flight information and the live photograph are not accessed or used by any other CBP systems. TVS does not further share or disseminate that information or use it for any other purpose beyond performing the TSA-requested facial identification operation.[277]

C. Data Retention

Data retention policies for the TSA FRT system differ between normal operations, described here, and a special data-collection mode used for system evaluation, described in more detail in the following subsection.

There are multiple sets of data handled by the system and multiple system components, so there are many details in the answer to the question of how long data is retained. There is a live photograph that is taken of the traveler at the airport for purposes of performing a comparison. For the 1:1 system, there is a reference photograph and associated biographic data taken from the identification document, plus biographic information and boarding information contained in the Secure Flight Passenger Data. For the 1:N system, in addition to the live photograph there is a gallery of photographs staged in TVS for comparison purposes. Data may also be held in the CAT device itself, in TVS, or in TSA's technical infrastructure that links systems. Images in the gallery and biographic data are drawn from other existing governmental holdings, and so even once they are deleted from TVS or TSA systems, the government still maintains the original data.

[276] *DHS/TSA/PIA-046(d) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, *supra,* at 3.

[277] *Id.* at 8–9.

The captured live photograph (for both 1:1 and 1:N systems) and data captured from the identity document (in the case of the 1:1 system) are deleted from the CAT-2 device when the TSO at the checkpoint begins the next traveler's transaction or logs off the device.[278] Secure Flight Passenger Data extracted from Secure Flight is retained securely by TSA's technical infrastructure for no longer than 24 hours after the flight departure time, to accommodate travelers who may require rescreening due to security events or who leave the sterile area for various reasons prior to their flight.[279]

In 1:N identification, the traveler does not provide an identity document to the CAT-2 device, so there is no initial capture of such information to be retained. The live photograph, returned potential match images, and biographic information and transactional metadata returned by TVS after a successful match are deleted from the CAT device when the TSO at the TDC either acknowledges the results or begins the next traveler interaction.[280] The gallery of templates remains in TVS for up to 24 hours after facial identification.[281]

There have been inconsistent statements regarding how long the newly captured live photo is retained when using the 1:N system. TSA has stated that for U.S. citizens, the live captured photo is deleted from TVS as soon as the identity verification process is complete and for non-U.S. citizens, the live photo is deleted after 24 hours.[282] TSA's official retention schedule for biometric screening, however, states that photos of all travelers, regardless of citizenship, are deleted from TVS within 12 hours, and TSA will delete passenger photographs from the technical infrastructure communicating with CBP TVS within 24 hours after a passenger's scheduled departure time.[283]

[278] *DHS/TSA/PIA-046(b) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Verification*, *supra,* at 3, 8.

[279] *Id*. at 8.

[280] *DHS/TSA/PIA-046(d) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, *supra,* at 8.

[281] U.S. Dep't of Homeland Sec., Transp. Sec. Admin. Response to Sen. Merkley Questions, at 3–4 (May 17, 2023).

[282] U.S. Dep't of Homeland Sec., Transp. Sec. Admin. Response to Sen. Merkley Questions, Attachment, at 3 (May 17, 2023). Note that in the cover letter, Administrator Pekoske also stated that "the photo taken at the TSA screening checkpoint is retained up to 24 hours to accommodate passengers that may require rescreening due to security events or when they decide to leave the airport sterile area for various reasons prior to their flight." This statement is apparently in error and refers to retention of the gallery images and passenger biographic data.

[283] *See* National Archives and Records Administration Records Schedule DAA-0560-2021-0001, TSA Biometric and Biographic Passenger Screening Records, https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0560/daa-0560-2021-0001_sf115.pdf.

D. Retention and Sharing for Testing and Evaluation Purposes

An exception to TSA's practice of not storing or saving information on the CAT device is when information is stored at specified times for "qualitative and quantitative analyses" to support testing and system improvements."[284] TSA has characterized this as part of a "continuous quality control process for the deployed technology in the operations and maintenance phase of its lifecycle."[285]

In comments to the press, TSA described this "limited testing environment" as a period of two to four weeks at "a few, specific locations."[286] During this time, the selected CAT-2 devices are configured to retain all collected traveler data, including information gathered from the identity document and the live image, for 24 hours.[287] Once per day during this testing period, TSA extracts the retained data and stores it on an encrypted hard drive.[288] It is then delivered to DHS S&T for analysis of system performance.

The information collected and shared with S&T includes a subset of traveler information from the ID, including the traveler's year of birth (but not date), photo associated with the identification document, and the live photo.[289] DHS S&T uses date of birth and sex to ensure that their analysis is capable of measuring the impact of those factors on performance. DHS S&T does not retain the traveler's name or any PII other than the facial image. DHS S&T may also make use of encrypted values that uniquely identify records that correspond to a particular traveler but cannot be used to match those records to the identity of that traveler.

S&T retains this data for up to 24 months in the TSA Cloud-Based Analytic Environment system.[290] This retention period is necessary to ensure that S&T can perform comparative testing between iterations of device configuration, algorithm version, or other system changes. These comparisons are used for regression testing and to evaluate how the updated

[284] *Id.*

[285] *TSA uses 'minimum' data to fine-tune its facial recognition, but some experts still worry*, *supra*.

[286] *Id.*

[287] TSA Responses to Third Round of PCLOB Questions, Q. 15(a) (Dec. 2023).

[288] PCLOB Phone Call with TSA and DHS (Feb. 9, 2024).

[289] *TSA uses 'minimum' data to fine-tune its facial recognition, but some experts still worry*, *supra*.

[290] PCLOB Phone Call with TSA and DHS (Feb. 9, 2024); TSA Responses to Fourth Round of PCLOB Questions, Q. 10(b) (Feb. 2024).

configuration affects outcomes.[291] All data is kept logically isolated and is only accessible by a limited number of authorized S&T personnel.[292]

S&T has stated that it has agreements in place with TSA to define what data TSA sends to S&T and how the data can be used. After the 24-month testing period ends, or if TSA requests earlier deletion, S&T destroys the data and provides a "certificate of destruction" to TSA for confirmation.[293]

E. Conclusion

Based on the information provided, in most cases TSA's collection of data appears to be tailored to accomplish the operational requirements of the program. The majority of data that TSA collects is limited to the minimum amount of information needed to determine the identity of individuals at checkpoints in a reliable fashion.

In most cases TSA's collection of data appears to be tailored to accomplish the operational requirements of the program. The majority of data that TSA collects is limited to the minimum amount of information needed to determine the identity of individuals at checkpoints in a reliable fashion.

TSA's retention policies for 1:1 verification and S&T testing delete PII and other sensitive data as soon as it no longer is necessary. The lack of any retention of images or identity information used during normal operation of the 1:1 system represents an ideal standard. Traveler PII from Secure Flight is retained in TSA's technical infrastructure for 24 hours to "accommodate travelers that may require rescreening due to security events or when they decide to leave the sterile area for various reasons prior to their flight,"[294] which seems to be a reasonable purpose for additional retention.

Ongoing testing is important to identify issues with accuracy and demographic performance, and to ensure that FRT use at the checkpoint continues to work as intended. Given the importance of this testing, TSA and S&T have established appropriate data collection and retention practices for the evaluation.

[291] PCLOB Phone Call with TSA and DHS (Feb. 9, 2024).

[292] TSA Responses to Fourth Round of PCLOB Questions, Q. 10(b) (Feb. 2024).

[293] *TSA uses 'minimum' data to fine-tune its facial recognition, but some experts still worry*, *supra*.

[294] *DHS/TSA/PIA-046(d) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, *supra,* at 8.

Data retention for 1:N operations presents more concerns. It is unclear why the live captured traveler photo remains in TVS and TSA's technical infrastructure for 24 hours and cannot be deleted immediately. In the event that a traveler needs to be rescreened, they would be required to take a new photograph for comparison to the TVS gallery. Any actions otherwise would present a risk of an impostor attempting to use the identity of someone who has already been approved to pass through the checkpoint. Aside from that concern, however, as currently configured, the limited forms of sharing of information with TVS for purposes of performing identification appear appropriate and necessary for the system to function.

VII. Safeguards Against Expansion or Misuse

Many of the privacy and civil liberties concerns raised by civil society groups focus not on TSA's current use of FRT, but rather on the broader risks and harms of government misuse of travelers' biometric information and the potential expansion of government use of FRT systems for new purposes or the misuse or abuse of the existing system. The use of FRT by authoritarian and repressive regimes abroad stands as a warning that broad use or abuse of this technology can curtail individuals' freedom of movement, association, and speech.[295]

As relates to TSA's use of FRT specifically, some have raised concerns that biometric or biometric-derived data collected or generated at the checkpoint could be misused, accessed by malicious actors, or used for other purposes. These concerns also include that, once developed and deployed, FRT systems could be used beyond TSA's stated purpose of aviation security.

This section examines existing and potential safeguards against misuse, unauthorized access to, or loss of biometric data, as well as possible future expansion of the purposes to which the technology is put. Reducing the amount of data collected and the extent to which the data that is collected is shared and retained is an important first step in preventing misuse and abuse; such practices are described in the previous section. Here, we discuss additional safeguards to prevent misuse, including training and personnel policies, regulatory and statutory limits on allowable purpose, forms of technical controls, and a program of audits and oversight functions to ensure that the use of FRT is consistent with these protections and the other limits described in earlier sections of this report.

A. Limits on Use and Purpose

In its public Facial Recognition Technology fact sheet, TSA states that FRT is "solely used to automate the current manual ID checking process and will not be used for surveillance or any law enforcement purpose."[296] This limitation is not directly enforced by any statutory language but is consistent with TSA's authority as a non-law enforcement agency and disclosures made by TSA in PIAs and SORNs. Although any change made by TSA to use their FRT systems for other purposes would at a minimum require public notice and comment in accordance with appropriate administrative procedures, there are few statutory limits that are specifically directed to the use of biometrics.

[295] *See* NAS FR Report, *supra*, at 1–3, 5 (stating that FRT "can be a powerful tool for pervasive surveillance" and that, among other dangers and potential abuses, these concerns were "not just abstract or theoretical.").

[296] U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Facial Recognition Technology, supra* (last visited Apr. 16, 2025).

The Privacy Act and the FIPPs include several safeguards regarding purpose specification to protect against the undisclosed expansion of the purposes to which a technology is put. The Privacy Act states that an agency must "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[297] Additionally, the FIPPs principle of use limitation dictates that "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."[298]

Under the Privacy Act, when federal agencies collect and store information about individuals and that information is retrieved by a personal identifier, they are required to publish a public System of Records Notice (SORN) that describes the purposes for collecting and using that information. The information cannot be used for other purposes without publicly modifying the SORN. DHS has stated that the information used by TSA's 1:1 and 1:N FRT systems qualifies for coverage under the Privacy Act and must be accounted for in SORNs.[299] Three published SORNs relating to DHS's broader transportation security and border security operations account for the information used as part of TSA's 1:1 and 1:N FRT systems, according to the department.[300]

Privacy Act-derived limitations on purpose are important but would not prevent TSA, or another component of DHS, from publishing new PIAs and SORNs that expanded the use of this data. Further, because the limitations focus on data, and not systems, the FRT systems themselves could be repurposed or expanded.

Many federal statutes and regulations directed to specific departments and applications limit the use of sensitive personal data to the purpose for which it was collected.[301] However, there are no comparable restrictions specifically directed to

[297] 5 U.S.C. § 552a(e)(1).

[298] *DHS Privacy Policy Guidance Memorandum 2008-01*, *supra*, at 4.

[299] *See* U.S. Dep't of Homeland Sec., *Privacy Threshold Analysis for Travel Document Checker Automation Using Facial Identification* (Apr. 3, 2024).

[300] *Id.* The three SORNs DHS has referenced are the following: DHS/TSA-019 Secure Flight Records, 80 Fed. Reg. 233 (Jan. 5, 2015); DHS/TSA-001 Transportation Security Enforcement Record System, 83 Fed. Reg. 43888 (Aug. 28, 2018); and DHS/CBP-007 Border Crossing Information, 81 Fed. Reg. 89957 (Dec. 13, 2016).

[301] *See, e.g.*, 13 U.S.C. § 9(a)(1) (prohibiting the Commerce Department from using census data "for any purpose other than the statistical purposes for which it is supplied," subject to certain exceptions); 26 U.S.C. § 6103 (generally prohibiting the disclosure by government employees of tax returns and "return information" received by the IRS, except as expressly authorized by law); 20 U.S.C. § 1232g(b)(1) (prohibiting certain educational institutions from releasing student educational records except for certain educational purposes or with the student or parent's written consent); 45 C.F.R. § 164.502 (Entities regulated by the Health Insurance Portability and Accountability Act may only use and disclose protected health information

biometrics that apply to TSA's use for aviation security. If the use of biometrics becomes more widespread, Congress may wish to consider specific restrictions on the use of biometrics, especially those of U.S. persons.

B. TSO Training and Policies

The risk of government misuse of travelers' biometric information is addressed in part by written policies and procedures for TSA and DHS personnel that define the appropriate uses of that information and the FRT systems. All TSA and contractor personnel are required by law and DHS policy to safeguard PII and SPII to prevent adverse consequences, such as a privacy incident, breach, or misuse of data.[302] The FIPPs principle of accountability and auditing dictates that "DHS should be accountable for complying with these principles" and "providing training to all employees and contractors who use PII."[303] To reinforce this, DHS requires all employees and contractors to complete an annual online privacy awareness training.[304]

TSA has stated that any biometric technology must be "highly useable for all passengers and operators, considering the diversity of the traveling public and TSO roles," and that TSOs are trained to treat passengers with respect.[305] According to TSA, TSOs receive mandatory training that includes information about travelers' ability to opt out of FRT.[306] TSA also provides training for specific roles relating to the TSO position, such as supervisory roles and system operator roles.[307] TSOs are required to complete four different CAT-2 training programs.[308]

According to TSA, all CAT-2 training material that has been released since December 2022 provides the TSOs with the following guidance for handling situations in which a

as permitted by regulation, such as for treatment, payment, and health care operations purposes, and, in general, may not sell such information.).

[302] *Handbook for Safeguarding Sensitive PII, Privacy Policy Directive 047-01-007*, *supra*, at 3–4.

[303] *DHS Privacy Policy Guidance Memorandum 2008-01*, *supra*, at 4.

[304] U.S. Dep't of Homeland Sec., *Privacy Training & Awareness*, https://www.dhs.gov/privacy-training (last visited Apr. 15, 2025).

[305] Transp. Sec. Admin. Response to Sen. Merkley Questions, at 2 (May 17, 2023).

[306] *Id.*

[307] PCLOB Phone Call with TSA and DHS (Feb. 9, 2024).

[308] Trainings include CAT-2 New User Training, CAT-2 Differences Training, CAT-2 Advanced Resolution Training for supervisory Transportation Security Officers, and the Train the Trainer training for security training instructors. Mandatory on-the-job training supplements these training programs. TSA did not supply information on how often TSOs must complete such trainings. U.S. Dep't of Homeland Sec., Transp. Sec. Admin, *Attachment 13: Biometric Training Opt-out for CAT-2 and TIS* (March 11, 2024).

traveler chooses to opt out of FRT: "If the individual does not want to take a photo allow the individual to opt out, turn the Camera off, use CAT to verify their ID, and Screening Type, verify the individual matches the photo on the CAT-2 Monitor, or the ID. Turn the Camera back on once that individual has finished at TDC."[309] There are graphics in the training to show TSOs how to turn the camera off and on, and the training shows the icons that are displayed on the TSO monitor and the traveler's monitor indicating that the camera has been turned off.[310]

Similarly, the TSA PreCheck Touchless ID training provides the TSOs conducting TDC with the following guidance concerning travelers' ability to opt out: "Any individual may decline to have their photo taken. If the individual does not want to take a [sic] participate, allow the individual to opt out and refer the individual to a TDC position using either a CAT unit or standard TDC operations."[311]

C. Technical Protections

In addition to federal agencies' obligation to implement risk assessment-based information security programs under FISMA,[312] DHS privacy policy guidance dictates that "DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure."[313] The technical architecture and implementation of the system also provide protections against misuse of data or violations of the various limits to use described above. Security features and choices can also reduce, but not eliminate, the risk of external malicious actors gaining access to the system or obtaining sensitive data.

In reviewing the technical protections in the CAT-2 system, PCLOB was given access to DHS and TSA documents containing Sensitive Security Information (SSI). While details from

[309] *Id.*

[310] *Id.*

[311] U.S. Dep't of Homeland Sec., Transp. Sec. Admin., *Attachment 13: Biometric Training Opt-out for CAT-2 and TIS* (March 11, 2024).

[312] The Federal Information Security Modernization Act of 2014 (FISMA) updates the federal government's cybersecurity practices to strengthen information security systems and creates a model for managing information security that is defined by standards developed by NIST. Under this statute, agencies are charged with providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by the agency or on behalf of the agency and information systems used or operated by or on the behalf of the agency. Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551 et seq.

[313] *DHS Privacy Policy Guidance Memorandum 2008-01*, *supra,* at 4.

these documents cannot be made public, nothing we reviewed changed our conclusions stated in this section. Based on our review of DHS's cybersecurity practices and issues, DHS has appropriately considered cybersecurity risk and adopted reasonable controls and measures to minimize such risk in the development of the program.

1. Access Controls

In situations where training is insufficient, or where employees may be acting outside the defined limits of their roles, certain technical measures can assist in preventing and detecting misuse.

TSA has implemented access controls in CAT-2 and related systems to ensure only authorized personnel may access biometric information.[314] The CAT-2 device hardware is locked when not in use and access to the system requires an active Personal Identity Verification card as well as personal identification number.[315] TSA personnel and contractors are assigned roles for accessing the system based on their function.[316] A system administrator grants authorized users access based on what capabilities and data they need to accomplish their role.[317] The Information System Security Officer (ISSO) confirms policy compliance and manages account and privilege activation or deactivation as necessary.[318]

2. Data Protection

In any system, encryption is one of the key ways in which data is protected against access by unauthorized individuals. TSA has stated that it encrypts all data at rest and in transit in compliance with mandatory federal data encryption standards. During 1:N operations, TSA also employs mandatory federal data encryption standards for all data in transit between the CAT device and CBP's TVS.[319] TVS retains information temporarily in a secure virtual cloud environment.[320]

[314] *DHS/TSA/PIA-046(d) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, *supra*, at 11.

[315] TSA Responses to Fourth Round of PCLOB Questions, Q. 6(c) (Feb. 2024).

[316] *DHS/TSA/PIA-046(d) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, *supra,* at 10.

[317] *Id.*

[318] *Id.*

[319] U.S. Dep't of Homeland Sec., Transp. Sec. Admin. Response to Sen. Merkley Questions, at 4 (May 17, 2023); *DHS/CBP/PIA-056 Privacy Impact Assessment for the Traveler Verification Service*, *supra,* at 26.

[320] *DHS/CBP/PIA-056 Privacy Impact Assessment for the Traveler Verification Service*, *supra,* at 26.

The use of templates to represent biometric images also provides some protection, although perhaps only of limited effectiveness. As described above, FRT works by converting live traveler facial images into mathematical representations called templates.[321] TSA has stated that "[e]xternal parties cannot reverse engineer these templates for viewing (meaning if an unauthorized user were to view the template, it would not be visible as a facial image)."[322] CBP concurred with TSA, assuring that "templates [in TVS] cannot be reverse-engineered for viewing by external parties."[323] CBP relies on representations from the vendor regarding reverse engineering and has not conducted its own testing of whether templates can be reverse engineered.[324]

Continuing research and advances in AI techniques indicate that templates may not be as secure as once believed. The 2024 NAS FR Report concluded that "[t]emplates are generally reversible … they can be reversed, with some difficulty, to something with some resemblance to the original face."[325] Ensuring templates are protected from disclosure is thus essential to protecting individual privacy. While the use of standard encryption provides protection to biometric data in transit and at rest, it does not protect it while in use. Therefore, DHS should continue to investigate how to further protect biometric templates or to use templates that have stronger protections against reversal.

D. Audits and Oversight

Limitations on use, access controls, training, and other mechanisms designed to prevent the misuse of FRT, or the data gathered or generated using FRT, are important to the protection of individual rights. However, public confidence in the effectiveness of these limitations requires regular, comprehensive, and transparent audits to demonstrate compliance. The FIPPs principle of accountability and auditing dictates that "DHS should be

[321] *Id*. ("Biometric templates are strings of multiple numbers that represent specified images and facilitate facial recognition matching within a secure environment.").

[322] Letter from David Pekoske, Administrator, Transp. Sec. Admin., to Sen. Jeff Merkley (D-OR), at 3 (May 17, 2023); *id*.

[323]*DHS/CBP/PIA-056 Privacy Impact Assessment for the Traveler Verification Service supra*, at 26, note 19; *see* CBP Office of Field Operations Email to PCLOB Staff (Aug. 2020).

[324] CBP Office of Field Operations Email to PCLOB Staff (Aug. 2020). Some research suggests the possibility of attacks that reverse engineer facial images from biometric templates. *See, e.g.,* Guangcan Mai et al., *On the Reconstruction of Face Images from Deep Face Templates*, at 99 (Apr. 29, 2018), https://arxiv.org/abs/1703.00832.

[325] NAS FR Report, *supra*, at 37; *see also* Hatef Shahreza & Sébastien Marcel, *Comprehensive Vulnerability Evaluation of Face Recognition Systems to Template Inversion Attacks via 3D Face Reconstruction* (Sept. 5, 2023), https://ieeexplore.ieee.org/document/10239446; Guangcan Mai et al., *On the Reconstruction of Face Images from Deep Face Templates* (2017), *supra*; Andrey Zhmoginov & Mark Sandler, *Inverting Face Embeddings with Convolutional Neural Networks* (June 14, 2016), https://arxiv.org/abs/1606.04189.

accountable for … auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements."[326]

Many aspects of TSA's use of FRT, including its 1:1 and 1:N pilots, have technical capabilities supporting audits and analysis of data access patterns. For example, the system owner and ISSO can analyze and audit system user access for Secure Flight and CBP TVS to ensure that only individuals with a need-to-know and an authorized purpose have accessed data contained in those systems.[327] The program manager "may audit the examination, maintenance, destruction, and usage activities to ensure they are carried out as described and that privacy and security protections are followed."[328]

DHS Directive 026-11 requires DHS S&T to review the technical performance of FRT systems every three years; however, the policy does not require that review encompasses privacy or compliance issues.[329] The Directive does require the Chief Privacy Officer to perform "periodic Privacy Compliance Reviews of DHS use of FR and FC [Face Capture] technologies to verify compliance with DHS privacy policy."[330] As yet, no such privacy review has taken place and TSA has not disclosed a schedule for such reviews, nor committed to disclosing the results of such audits and any acts of non-compliance to oversight entities.

E. Conclusion

Based on our review of DHS's cybersecurity practices and issues, DHS has appropriately considered cybersecurity risk and adopted reasonable controls and measures to minimize such risk in the development of the program. However, given potential developments in the reversal of biometric templates, we recommend that DHS investigate techniques for generating more secure templates or for better protecting templates while in use.

Overall, given the current technical architecture and DHS policies regarding information retention and sharing, the 1:1 system presents a relatively limited risk of expansion or misuse. Clearer policies, regulatory, or statutory limitations, alongside a system of established oversight, logging, and audits, would reinforce public confidence that the system is used only for its designated purpose. Any further expansion of the scope or application of TSA's use of FRT should come only after a determination that the benefits of

[326] *DHS Privacy Policy Guidance Memorandum 2008-01*, *supra,* at 4.

[327] *DHS/TSA/PIA-046(d) Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, *supra,* at 10.

[328] *Id.* at 11.

[329] DHS Directive 026-11, *supra*, at 5–6. As noted above, however, DHS has not confirmed that DHS Directive 026-11 is currently in force.

[330] *Id*. at 4.

such expansion outweigh the increased risks to privacy and civil liberties, as well as full public disclosure and debate.

As described in Section VI.B., the default system configuration for 1:1 identity verification does not retain information that would be available to other entities, such as law enforcement, after the fact. The biometric information collected at the checkpoint only includes information required for verifying traveler identity and, in limited circumstances, assessing operational and technological components for testing and evaluation purposes. Further, the implementation of the 1:1 identity verification system does not readily lend itself to wider uses. Strictly comparing an identity document with an individual establishes only that the identification document corresponds to the person presenting it. Accordingly, it would not be an effective tool for identifying wanted criminals, for example.

The 1:N program offers more opportunities for potential expansion and for that reason has greater potential privacy and civil liberties implications. The 1:N program retains information within TVS only for a limited time and only for the purpose of determining whether a person presenting themselves at the checkpoint can be matched to a gallery of individuals who are traveling that day. However, 1:N systems could be more easily adapted to identify individuals drawn from a larger set of people of interest. If TSA were to expand the use of the program to a wider population, the 1:N configuration could raise more significant privacy and civil liberties concerns, given the system's potential for accessing more biometric data drawn from other government databases.

VIII. Conclusions

Government programs that employ FRT to recognize members of the public should justify the benefit gained by employing it, operate transparently, and provide robust protection against the risks to the public's privacy and civil liberties. Use of FRT has raised concerns due to its potential for use in the surveillance of public spaces, the sensitivity of the biometric data required to operate it, and documented patterns of uneven, albeit improving, demographic performance. However, as this report discusses, these risks are significantly mitigated for TSA's current FRT program.

As both the 1:1 and 1:N systems are new and have evolved during program development, there is not yet established evidence of their operational value. However, initial results do suggest that they operate with high accuracy and assist in increasing the rate at which travelers are authenticated and pass through security. Given TSA's existing security approach of facilitating screening for trusted travelers, adding FRT appears to improve the reliability and speed of the program. The 1:N program is potentially more convenient for travelers because they are not required to present an identity document; in part because of that, identity determination may be accomplished more quickly compared to manual procedures or using 1:1 FRT. But those advantages are difficult to measure and would need to be weighed against privacy and civil liberties concerns we have discussed.

Use of FRT has caused concern due to its potential for use in the surveillance of public spaces, the sensitivity of the biometric data required to operate it, and documented patterns of uneven, albeit improving, demographic performance. However, these risks are significantly mitigated for TSA's current FRT program.

Despite the low overall error rate that remains, TSA has continued to observe some demographic differential performance. Even if the impact of false negative results is relatively minor, the volume of travelers that could be affected provides reason for TSA to continue to measure and improve both overall performance and accuracy as well as demographic differences in performance.

The use of biometric data in the 1:1 system represents a nearly ideal case of data protection; the live image and image from the identity document are retained only for the few seconds needed to compare them, then are deleted. The 1:N system presents a more extensive system of collecting images for staging and retaining them for 24 hours. We recommend that TSA and CBP continue to make efforts to implement policy, operational, and technical protections against data loss or misuse.

TSA should continue to operate both programs such that participation remains voluntary under current circumstances. While opt-in is inherently less intrusive than opt-out, it may be that for logistical reasons, 1:1 can only operate successfully as an opt-out program. In such a case, however, it is all the more important that travelers are fully aware of the rights to opt out, and that such a decision is consistently respected by TSOs. Both elements will require more consistent effort by TSA to provide clear notice and training.

TSA should continue to operate both the 1:1 and 1:N systems such that participation remains voluntary under current circumstances. While opt-in is inherently less intrusive than opt-out, it may be that for logistical reasons, 1:1 can only operate successfully as an opt-out program.

There are undeniable challenges with public notice and disclosure for programs in development that change over time. However, TSA must provide more comprehensive, accurate, and timely descriptions of the program, and to the extent possible, disclosure of the planned system. Categorizing operational systems that process large numbers of travelers as “pilots” or “proofs of concept,” in some cases for more than five years, is confusing at best.

TSA has incorporated important safeguards designed to ensure that its 1:1 system is a responsible and effective use of FRT in support of legitimate and important purposes with minimal risk of abuse or misuse. Our recommendations are designed to assist TSA in achieving that result.

While the 1:N system continues to be considered in the development and evaluation phase, and may operate differently in the future, expansion or modification of the 1:N program would require further analysis of the risks and benefits.

PART 3:
RECOMMENDATIONS

I. Overall Program

Recommendation #1:

TSA should collect and publish usage and performance data for program evaluation.

An assessment of the impact and effectiveness of the program begins with an accounting of key metrics of performance, including overall volume, efficiency, successful uses of the technology, and the frequency, types, and causes of failures.

At a minimum, this data should include how many travelers were processed with either 1:1 or 1:N FRT systems, how many were processed by manual TSO matching, how many travelers chose to opt out, how many travelers for whom the system reported a non-match but were subsequently confirmed by the TSO (i.e., false negatives), and the number of travelers correctly determined to not match their identification document (i.e., impostors). While the systems are not currently configured to collect this data, we are not aware of technical reasons why the data could not be collected during operations. While metrics covering the operation of the entire program would be the most comprehensive measurement, it may be that statistical sampling through observational studies may be more economical or practical. As only summary-level statistics would be gathered, there would be no additional personal information retained. TSA should work with the vendor to add this capability to the software or otherwise establish a mechanism for collecting such data.

Further, TSA should collect data, either through post-hoc data analysis under TSA's agreement with DHS S&T or statistical sampling of observational studies, on the rates of false negatives on different demographic groups. DHS should ensure that any process of data collection and analysis for demographic performance includes privacy protections built in throughout the process, including provisions to ensure demographic data is not tracked in a way that is linkable to individuals.

TSA and DHS should release this data to appropriate internal and external oversight bodies and, to the extent possible consistent with national security, to the public. Congress should consider requiring regular reporting of this data, but even if Congress does not act, TSA should prepare and publish such data for release, consistent with national security.

II. EFFECTIVENESS AND VALUE

RECOMMENDATION #2:

TSA should perform operational testing of the ability of both human officers and the FRT systems to detect impostors. TSA should report the results of this testing to appropriate oversight bodies, and to the public to the extent practicable.

As discussed in Part 2, DHS's testing of the FRT systems' ability to flag individuals who do not match their documents (for 1:1) or reference photos in the gallery (for 1:N) has occurred to date using technology or scenario testing. We are not aware of operational tests that have evaluated how effectively TSOs spot individuals who do not match their identity documents. Measures of performance of both TSOs on their own and TSOs working in conjunction with FRT systems could yield information about comparative efficacy while also providing TSA with important data to inform the FRT program as it continues to develop.

TSA has performed covert testing at operational security checkpoints to measure the vulnerability of other TSA security processes and practices against threats, such as attempts to smuggle guns or explosives on board an aircraft.[331] Covert testing can identify shortcomings in procedures or practices that, when addressed, improve the effectiveness of the checkpoint.

TSA considers identity verification an important aspect of its security architecture. If potential impostors were to successfully pass through the document checker component of security checkpoints undetected, they would gain access to passenger terminal areas and aircraft without having been evaluated as potential risks to security. Given the security risks associated with unauthorized access, we recommend that TSA expand the scope of covert testing to assess the feasibility of such attempts and the efficacy of both the FRT systems and human officers in recognizing such attempts. TSA should use the information gathered in such tests to evaluate the overall capability of their FRT systems as well as the performance of individual checkpoint operators and officers.

[331] In the past, TSA has conducted covert tests of newly deployed technologies, such as TSA's Advanced Image Technology, of passenger screening canine teams, of transportation worker credential (TWIC) holders, and others. *See, e.g., Identifying, Resolving, and Preventing Vulnerabilities in TSA's Security Operations: Hearing Before the H. Comm. on Oversight and Reform*, 116th Cong. 3–4 (June 25, 2019) (statement of TSA Administrator David P. Pekoske).

TSA should publish a report on the results of these impostor detection tests to inform policymakers and the public with as much detail as possible, consistent with national security. Disclosing those results publicly could help to enhance public trust by improving transparency, combating suspicion and incorrect information, and facilitating informed public discourse. To aid in the reliability and neutrality of the testing, TSA should consider requesting that an agency external to DHS conduct the tests and analysis.

III. DEMOGRAPHICS AND CONSEQUENCES OF MISIDENTIFICATION

RECOMMENDATION #3:

DHS should establish standards that define minimal differential demographic performance of FRT systems and require vendors or internal developers to employ techniques that minimize such differentials.

Differential demographic performance can stem from multiple causes, including algorithm design, incomplete or unrepresentative training data, system component performance, and other factors.

DHS, in consultation with NIST and other relevant government agencies, should work to establish appropriate metrics and standards in order to minimize differential demographic performance to the greatest extent possible and to identify development, training, and deployment practices in accordance with that objective. For example, differential demographic performance can stem from the use of training data containing an insufficiently representative sample of racial, ethnic, age, or gender groups.

When acquiring an FRT capability from vendors or developing one internally, DHS should require that vendors meet the established standards and follow best practices for developing and training systems in order to minimize or eliminate differential demographic performance. Such performance and practice should be explicit requirements included in public solicitations for proposals and used as a factor in evaluating such proposals. DHS should publicly disclose these standards and establish procedures for remediation if systems fall below those standards when deployed.

RECOMMENDATION #4:

TSA should require FRT vendors to document information about the algorithm and training data employed and make that information publicly available to the extent possible consistent with national security.

Whenever a TSA system incorporates facial recognition that will be used to identify members of the public, TSA should publicly disclose details about the algorithms being used, including information about the algorithms' identity and version, updated as necessary; information about the training sets employed; and assessments of demographic performance, to the extent possible consistent with national security.

TSA and DHS should only review submissions of FRT products, or internally developed systems, if the algorithm has been submitted to NIST's FRTE[332] and tested for the appropriate mode for which the product or system is being considered. Further, as vendors or internal developers update algorithms, each meaningful iteration should also be submitted to FRTE before DHS deploys them to production systems. DHS should further work with NIST to ensure that the specific names and identifiers of algorithms and versions used in public disclosures match those used by NIST.

[332] *See* Nat'l Inst. of Standards and Tech., *Face Technology Evaluations - FRTE/FATE*, https://www.nist.gov/programs-projects/face-technology-evaluations-frtefate (last visited Apr. 4, 2025).

IV. TRANSPARENCY

RECOMMENDATION #5:

TSA should regularly obtain independent assessments of staff compliance and the effectiveness of signage and training policies and practices.

TSA signage and employee interactions are key elements in providing travelers with accurate and timely notice of their rights regarding their interactions with TSA's FRT systems.

Given the difficulty of successfully conveying information in airport terminals, we recommend that TSA regularly assess the effectiveness of FRT-related signage and notice mechanisms, including the training and procedures for officers or other TSA employees in informing the public. The results of such assessments should inform TSA's efforts to revise elements of signage and training standards. This review should also consider any other means by which TSA informs travelers of their rights, including pamphlets and audio announcements.

TSA should track staff compliance with training and procedures as they relate to the operation of FRT systems. Training should be updated regularly to account for any changes in technology or processes. If data from traveler complaints or TRIP indicate patterns of deviation from these procedures or other issues, TSA should update its training accordingly.

RECOMMENDATION #6:

TSA should issue a comprehensive PIA and other privacy disclosures for the FRT programs.

TSA should publish a fully updated, comprehensive PIA that lays out the complete current status of TSA's use of FRT in airports. The current PIA series has five iterations, and it is not clear which accurately reflects the current system that travelers may encounter. The new PIA should replace the existing assessments and should clearly describe how TSA uses FRT, both in 1:1 and 1:N operations. The DHS PIA website should also make clear that previous FRT PIAs are no longer current and have been superseded.

Further, TSA should publish an additional PIA that lays out the complete expected future status of TSA use of FRT in airports if or when the 1:N program is determined to no longer be in a development or evaluation stage.

TSA should ensure that it publishes PIAs and other privacy disclosures for FRT programs as soon as privacy risks are identified, even if programs are still in pilot phase or are otherwise still being developed. The E-Government Act of 2002 requires agencies to conduct a PIA before "developing or procuring IT [information technology] systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public."[333] Per OMB guidance regarding PIAs,[334] PIAs published at this stage should include discussions of privacy impacts from systems in development. Given the privacy-sensitive nature of FRT, TSA should be proactive in publishing privacy compliance documentation.

While changes to the system's purpose would have to be reflected in an updated or new PIA, DHS often waits until after systems have been deployed to publish PIAs. Applicable OMB guidance requires updates "as necessary where a system change creates new privacy risks" and "to reflect changed information collection authorities, business processes or other factors affecting the collection or handling of information in identifiable form."[335]

Further, if TSA makes significant changes to the technical infrastructure or configuration of the CAT-2 devices, or the technical system that supports their operation, TSA should notify the public describing these changes, the purpose for them, and the consequences of them, even if TSA otherwise believes that the changes would not create new privacy risks that would require an update to the applicable PIAs or existing public program disclosures.

As PIAs can be technical, TSA should also ensure that the description of the FRT programs on its website includes clear disclosures of the ways in which facial images are collected, stored, and used, written in straightforward, non-technical language.

[333] *See* Pub. L. 107-347, § 208, 116 Stat. 2921 (2002).

[334] *See* Off. of Mgmt. and Budget, Exec. Off. of the President, *OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 2003), https://obamawhitehouse.archives.gov/omb/memoranda_m03-22/.

[335] *Id.*

RECOMMENDATION #7:

TSA should define and use consistent terminology to describe the deployment status of its systems.

TSA and DHS should re-evaluate their processes for labeling the use of a system in real-world operations as a "pilot." For many years, TSA has categorized the FRT systems as a "proof of concept" or "pilot." However, the FRT systems are increasingly being used to screen travelers in the ordinary course of operations. In reviewing the status of the program in 2023, TSA concluded that it was not "a small scale, short-term experiment," that it was intended for future broader deployment, and that it was performed as part of an existing contract with service providers, which suggest that the program should no longer have been considered a pilot at that point in time.[336]

Further, DHS should avoid using the term "proof of concept" to describe ongoing operational programs that affect travelers. Though DHS/TSA have used the term in public-facing documents, such as PIAs, the term is not defined in the DHS Lexicon. Upon PCLOB's inquiries into its meaning, DHS/TSA could not provide a definition of this term nor differentiate between the programmatic implications of a proof of concept versus a pilot program. If DHS finds it necessary to refer to a particular stage of testing and development that is distinct from "pilot," it should clearly define it in the DHS Lexicon and the appropriate acquisition procedures and manuals.

[336] *See* IDM Section 107 Memo, *supra*.

V. Individual Participation

Recommendation #8:

TSA and DHS should establish procedures for collecting, investigating, and responding to FRT-related inquiries and complaints from travelers.

DHS and TSA should ensure that systems that offer opportunities for the public to register comments or complaints regarding airport security experiences, such as public web input forms and phone prompts provided by TCC and TRIP, include options relating to FRT and biometrics specifically. All such public input should be routed to a specific office or agency element tasked with processing, responding to, and analyzing it. TSA should develop specific procedures for handling such inquiries, including providing useful feedback to travelers and following up with TSA staff and management at particular airports to investigate issues that may be prompting such complaints. TSA should include information on how to contact appropriate redress services on all information sources relating to the use of FRT, such as public signage, ticket information, and communications from TSA.

TSA should track these traveler inquiries and complaints over time to identify patterns of concern, such as accuracy for particular demographic groups or effectiveness of signage or employee training. TSA should develop and implement additional procedures to remediate any such identified issues.[337] We recommend that DHS ensure that appropriate offices have sufficient staff to perform these functions.

[337] *See* U.S. Gov't Accountability Off., *TSA Should Assess Potential for Discrimination and Better Inform Passengers of the Complaint Process*, at 32–33 (Nov. 2022), https://www.gao.gov/assets/d23105201.pdf.

VI. COLLECTION, SHARING, RETENTION, AND USE OF DATA

RECOMMENDATION #9:

TSA should not retain live photographs beyond the minimum amount of time necessary to perform matching.

Data minimization is essential to protecting sensitive personal information from breach or loss. Consistent with established principles of data minimization, TSA's FRT systems should store biometric data only as long as it is necessary for their function (i.e., to determine the identity of a traveler at the checkpoint).

The 1:N program, which is still being evaluated by TSA, retains newly captured images for 24 hours. TSA has not provided to PCLOB a mission justification for the benefits of this period of retention. TSA should perform an analysis to determine the minimum amount of time that images need to be retained to accomplish mission needs and delete images after that amount of time, and provide the results of that analysis to appropriate oversight bodies.

RECOMMENDATION #10:

TSA should configure the CAT-2 devices to perform privacy-enhancing operations locally.

In the current FRT configuration, multiple operations that can preserve privacy, such as removing or obscuring personal information, are performed outside of the CAT-2 device. For example, live photographs taken by the CAT-2 device are transmitted to TVS, where a template is created from the photo. Similarly, during evaluation, data is removed from the CAT-2 device and then de-identified such that only traveler year of birth, traveler sex, identification document photograph, and live photograph are transferred to DHS S&T. Because each of these steps includes copying sensitive personal information from the device, they can create some risk of personal data being misused or improperly accessed.

To the extent possible, TSA and IDEMIA should modify CAT-2 software operations to add the capability of locally calculating templates compatible with TVS. This will require cooperation from NEC Corporation and TVS, but such a modification should be technically feasible. Similarly, TSA and IDEMIA should develop and install software onto the CAT-2 devices to perform the data de-identification, packaging, and encryption for evaluation purposes. Executing this process on the device will remove the need to export non-deidentified data.

VII. SAFEGUARDS AGAINST MISUSE

RECOMMENDATION #11:

DHS should either restore DHS Directive 026-11 to the website and affirm that it remains controlling policy, or commit to timely reissue an analogous policy.

Much of the foundations of the assurance that TSA will employ FRT in ways consistent with the protection of privacy and civil liberties, including the goal of minimizing bias in FRT systems and rights to opt out, were based on the policies set forth in DHS Directive 026-11. However, that directive is no longer available on DHS's website, and DHS was unable to confirm to PCLOB whether it remains official policy or not. A cornerstone of policy analysis is that rules that define allowed and prohibited uses of systems must be clear and unambiguous. If DHS cannot state whether a given policy is in force or not, oversight agencies, operators, and the public cannot know what is allowed and what is not.

We recommend that DHS restore DHS Directive 026-11 to the departmental website and publicly affirm that it is controlling policy. Absent that, we urge DHS to quickly issue a new analogous directive.

RECOMMENDATION #12:

TSA, or an independent third party, should conduct regular, comprehensive audits to track compliance with privacy and civil liberties policies and procedures and evaluate their adequacy and sufficiency. TSA should make the results of such audits available to oversight bodies and, to the extent possible, to the public.

Under the DHS Directive on Facial Recognition Technology,[338] FRT systems must be tested and evaluated to establish whether they meet performance metrics and comply with international technical standards. TSA has not committed to performing regular audits that establish compliance with privacy and civil liberties protections.

We recommend that TSA establish a requirement for such audits and a regular schedule of performing them. These audits should include, at a minimum, identification of incidents of non-compliance with policies, any records of misuse or unauthorized access to personal

[338] DHS Directive 026-11, *supra*.

information, and evidence that the systems are used only in accordance with stated purposes.

TSA and DHS should release the results of these audits and reviews to appropriate oversight bodies and, to the extent possible consistent with national security, to the public.

RECOMMENDATION #13:

DHS S&T should assess the security and privacy risks associated with the potential to reverse engineer biometric templates and identify methods to mitigate these risks. In particular, DHS S&T should investigate the applicability of privacy enhancing technologies for securely creating, processing, storing, and querying biometric templates.

Increasing evidence suggests that biometric templates, the mathematical representations of facial images used by facial recognition comparison algorithms, are potentially susceptible to reverse engineering by malicious actors (that is, producing close approximations of the original images from which the biometric templates are generated). DHS S&T, in cooperation with NIST and other federal agencies, should investigate the potential for such attacks against templates used by algorithms employed by TSA, including the algorithm used in CBP's TVS for 1:N recognition, and identify methods that could mitigate those risks.

If researchers identify template-generation techniques that are more resistant to reverse engineering, or improved privacy-preserving methods for performing computations on templates (e.g., the ability to compare two encrypted templates), TSA should require FRT vendors to employ those improved techniques to the extent possible.

APPENDIX A: SEPARATE STATEMENT OF BOARD MEMBER BETH A. WILLIAMS

I commend the professional staff at the Privacy and Civil Liberties Oversight Board who have worked for many years on the factual investigation, analysis, and recommendations that today make up this report. This project was opened in June 2019, and publication has been almost six years in coming, spanning numerous Boards and incorporating the work of many present and former staff members. I am pleased that the results of their diligent effort are finally being publicly released, accomplishing an important part of the agency's mission to inform TSA's future operations and provide valuable transparency on a program that impacts privacy and civil liberties. I add this separate statement to highlight some matters in my individual capacity as a Member of the Board.

<u>Facial Recognition Should Remain Voluntary.</u>

I agree with the staff, and endorse their conclusion, that TSA's facial recognition program should remain voluntary for all passengers. Travelers should retain the ability to opt out of 1:1 facial recognition without penalty or additional burden, such as being required to wait in a longer or separate line. While FRT programs provide certain advantages to travelers, such as a streamlined checkpoint process and potentially safer flying experience, a traveler may decide—for any reason or no reason—not to participate in automated facial recognition.

<u>The Appropriate Comparison to Facial Recognition Technology Is Human Review.</u>

When evaluating this program, one must consider the true alternative: manual human identity matching. After the attacks of September 11, 2001, no reasonable person would argue that the government should *not* confirm the identity of those boarding aircraft. The alternative to FRT, then, is a return to the sole use of human Transportation Security Officers (TSOs) to perform a visual comparison between travelers and their identification photos.

In reviewing the available studies, PCLOB's staff concluded that "in similar contexts FRT is at least as accurate as, and very likely superior to, human performance." (*See* Report, *supra* at 49.) Indeed, "[g]iven humans' own lower accuracy at performing face matching for demographic groups other than their own or for unfamiliar faces, FRT systems very likely surpass human performance even considering demographic differential performance of such systems." (*Id.* at 51.) But FRT in its current iteration is not without its flaws, as the Report likewise details. When considering FRT's efficacy, policymakers must evaluate not only its imperfections, but whether it is superior to manual human review. This is why the report wisely recommends operational testing of the ability of both human officers and the FRT systems to detect impostors.

<u>Privacy and Civil Liberties Impacts Almost Entirely Result from False Negatives, Not False Positives.</u>

In discussing demographic differentials, the Report concludes that "[t]he absolute magnitude of the differences has decreased along with overall improvement in the performance of algorithms, but has not disappeared." (*Id.* at 71.) I support the Report's recommendations aimed at minimizing differential demographic performance to the greatest extent possible.

An informed discussion of the impacts, however, requires understanding that for privacy and civil liberties purposes, false negatives pose a far greater burden to affected individuals than false positives. To restate what has been explained in the Report, in the current 1:1 system, a false positive occurs when the system concludes there is a match between the traveler and her identification document image, *when in fact the two are not the same*. For example, a false positive would allow a traveler through security when using her cousin's driver's license. As the Report states, "In the context of the use of FRT in TSA's security system, false positives generally would not inconvenience legitimate travelers, but could present a security issue if they allow individuals who should not be allowed access to the secure area to proceed through security." (*Id.* at 2.)

False negatives, by contrast, occur when the system fails to match a person's live image to the facial image on her own document. That is, the system concludes there is no match, *when in fact the two are the same*. "False negatives primarily represent an inconvenience to the user attempting to establish their identity, such as a traveler." (*Id*. at 19.) When certain demographic groups have higher false negatives than other groups, that presents an unequal burden.

In the section of the Report on demographic differentials, particularly the portions explaining the 2019 NIST study, the discussion focuses almost exclusively on false positives. But that is confusing especially because, when applied to TSA's current 1:1 system, it would mean more older individuals and individuals from certain minority groups would be getting *through* security when they should not be, relative to other groups.

For purposes of understanding relevant demographic differentials for this Report, the most important numbers are the false negatives for the actual algorithms used by TSA. As the Report states, "[f]or false negatives, IDEMIA's most recent algorithm showed a differential of 1.09 times between the group with the highest rate (West African individuals at 0.21%) and the average across demographic groups. In other words, West African individuals could experience false negative results 9% more frequently than the average of the overall population." (*Id.* at 69.) However, the average error rate for the overall population is quite small. "Overall, the system correctly matched 99.4% of participants, and 99.9% of those participants for whom the system successfully acquired both a live image and the image from their presented identification document." (*Id.*) TSA should continue to take steps to minimize differential demographic performance to the greatest extent possible, especially with regard to false negatives.

<u>TSA Should Explore the National Security Benefit and the Privacy and Civil Liberty Risks of Comparison to Images of Known and Suspected Terrorists on the Watchlist.</u>

It may come as a surprise to many that TSA's FRT program currently has no connection to the Terrorist Watchlist. Instead, TSA's facial recognition technology is used *only* for verifying that a traveler's live image at the security checkpoint matches the image on the identity document he presents. A traveler may assume, when he chooses to submit to FRT at an airport security checkpoint, that his image, and the images of those fellow travelers on his flight who similarly participate in FRT, are compared against images of persons on the Terrorist Watchlist. That is not the case. In neither the standard 1:1 system, nor the opt-in 1:N system, are passengers' images compared against images of Known and Suspected Terrorists (KSTs).[1]

This knowledge may be important for passengers who choose to participate in FRT on the assumption that they are getting significant security benefit from doing so. Certainly there is some security benefit, as the report explains, by a system that better filters out impostors—those traveling under the photo identification of another person.[2] But that value

[1] Passengers' names and other identifying information are screened against the Terrorist Watchlist, but this is separate from FRT.

[2] Currently the FRT system flags instances where the live image of a person at the airport does not match the photo on the identification document the person has presented (i.e., a person trying to use his cousin's

is limited, and could potentially be magnified by comparing live images of travelers to a fixed gallery of images of persons on the Terrorist Watchlist. Using the information already held by the government to prevent potential future terrorist attacks was, of course, one of the most important recommendations of the 9-11 Commission, which warned, "The U.S. government has access to a vast amount of information…But the U.S. government has a weak system for processing and using what it has."[3]

TSA should therefore explore the technical feasibility, the expected national security value, and the potential scope of the resulting privacy and civil liberties impositions of enabling its FRT programs to compare the live photos of travelers against photos of individuals who appear on the No-Fly and Selectee List subsections of the Terrorist Watchlist.[4] As the Report discusses, aggregation of biometric data by the government can lead to misuse, compromise, and inaccuracies. Such a system may also increase the possibility of false matches—in this scenario, an innocent traveler being matched with the facial image of a known or suspected terrorist. The potential impact in such a situation could be far greater than the inconvenience the current system would impose. It would therefore be wise to conduct a thorough evaluation of both the advantages and disadvantages for national security and privacy and civil liberties before any action is considered.[5] To date, TSA has stated that they have not conducted any research into such a comparison feature.[6] Altering the program in such a manner ultimately may not be warranted, but the benefits and risks should be evaluated.

driver's license). But the FRT system would *not* flag instances where the live image of a person at the airport does match the photo on the identification document the person has presented (i.e., a valid ID with a photo of the actual traveler that nonetheless represents a false identity, such as assumed name). A person who knows or suspects that he is on the Terrorist Watchlist would likely try to travel under an assumed name with an identification document that matched that name (that is, it would be fraudulent because the person is not who the identification says he is, but it would be valid because it was issued by the government to traveler under his false identity). In the current 1:1 system in which the live photo of the traveler is compared only to the document he presents, such a deception would work. If the traveler's facial image were compared to images in a gallery composed of photos of persons on the No Fly List and Selectee lists, however, the traveler could be detected.

[3] Thomas H. Kean & Hamilton H. Lee, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks on the United States, at 416-417 (2004).

[4] For example, TSA should estimate what percentage of false positives would be anticipated by such comparison, and what impacts that could have when spread across the entire flying population, as well as any potential vulnerabilities from terrorists exploiting the opt-out feature.

[5] This should include any potential mitigations to privacy and civil liberty impacts, such as requiring that the gallery of Terrorist Watchlist photos be composed only of high-quality images.

[6] TSA Briefing to PCLOB, Sept 26, 2024.

APPENDIX B: GLOSSARY OF ACRONYMS AND ABBREVIATIONS

ACRONYM	DESCRIPTION
AI	Artificial Intelligence
ATSA	The Aviation and Transportation Security Act of 2001
CAT	Credential Authentication Technology
CBP	U.S. Customs and Border Protection
CRCL	DHS Office for Civil Rights and Civil Liberties
DHS	U.S. Department of Homeland Security
DHS S&T	DHS Science and Technology Directorate
FOC	Full Operational Capability
FRT	Facial Recognition Technology
FRTE	Face Recognition Technology Evaluation
FRVT	Facial Recognition Vendor Test
FY	Fiscal Year
GAO	U.S. Government Accountability Office
HART	Homeland Advanced Recognition Technology
ISSO	Information System Security Officer
KTN	Known Traveler Number
ML	Machine Learning
NIST	National Institute of Standards and Technology
OBIM	Office of Biometric Identity Management
OIG	Office of Inspector General

ACRONYM	DESCRIPTION
OPM	U.S. Office of Personnel Management
PCLOB	Privacy and Civil Liberties Oversight Board
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
SFPD	Secure Flight Passenger Data
SPII	Sensitive Personally Identifiable Information
SSN	Social Security Number
TCC	TSA Contact Center
TDC	Travel Document Checker
TRIP	DHS Traveler Redress Inquiry Program
TSA	Transportation Security Administration
TSO	Transportation Security Officer
TVS	Traveler Verification Service