COMPLY TO FLY?

How Airport Travelers Experience TSA's Facial Recognition Experiment

Algorithmic Justice League

Dr. Joy Buolamwini
Sushma Raman
Andrea Dean

July 2025

ACKNOWLEDGEMENTS

The TSA scorecard data for this report was assembled over two years by Algorithmic Justice League & Stanford AI Policy Program 2023 Summer Interns under the supervision of Tawana Petty and AJL AI Researchers Raymond Berger, Joy Buolamwini, Andrea Dean, and Aurum Linh. Special thank you to Gail Leibowitz for facilitating data gathering during holidays. Thank you to the University of Oxford Accelerator Fellowship Programme at the Institute for Ethics in AI for supporting the distribution of this Algorithmic Justice League-led report.

ABOUT ALGORITHMIC JUSTICE LEAGUE

The Algorithmic Justice League (AJL) is on a mission to raise awareness about the impacts of AI, equip advocates with empirical research, build the voice and choice of the most marginalized communities, and galvanize researchers, policy makers, and industry practitioners to mitigate algorithmic harms and biases.

At AJL, we believe respect isn't just about being recognized or not recognized. It is also about having agency regarding the processes that govern our lives. As companies, governments, and law enforcement agencies use AI to make decisions about our opportunities and freedoms, we must demand that we are respected as people.

To learn more about Algorithmic Justice League, visit www.ajl.org.

Cite as: Joy Buolamwini, Sushma Raman, and Andrea Dean, "Comply to Fly?: How Airport Travelers Experience TSA's Facial Recognition Experiment", Algorithmic Justice League, July 21, 2025, https://ajl.org/flyreport

TABLE OF CONTENTS

EXECUTIVE SUMMARY 2

1. INTRODUCTION 5

2. BACKGROUND AND CONTEXT 9

3. HOW IS TSA USING FACIAL RECOGNITION? 14

4. SUMMARY OF FINDINGS 20

A. Data Breadth & Demographics 20
B. Program Transparency 22
C. Consent 27
D. Treatment 35
E. Concerns 38
F. Program Benefits 43
G. Pre and Post-Operational Changes 44

5. DISCUSSION 48

6. RECOMMENDATIONS 55

#1 Preserve Freedom and Privacy 57
#2 Promote Informed Public Decision Making 58
#3 Prevent & Redress Disrespectful Treatment 59

REFERENCES 60

APPENDICES 65

APPENDIX A. PCLOB Report Recommendations 65
APPENDIX B. Glossary 67
APPENDIX C. AJL Survey Questions 71
APPENDIX D. Full List of Survey Airports 72
APPENDIX E. Tags for Manual Data Annotation 78

EXECUTIVE SUMMARY

Algorithmic Justice League (AJL) is issuing the **Comply To Fly?** report focused on the facial recognition program operated by the Transportation Security Administration (TSA). The primary timeframe for the report is the launch of the operational period (March 1, 2024) until June 2, 2025. While TSA initially described this program as a pilot, it has been expanding–to over 250 domestic airports as of the date of issuance of this report with plans to expand to 430 airports in the coming years. The report fills a critical gap in public knowledge about travelers' lived experience of encountering airport face scans.

Facial recognition technologies (FRTs) refer to a number of ways human faces are scanned to derive biometric information; the program used at TSA includes both facial verification (1:1 matching at TSA Security Checkpoints) and facial identification (1:N matching at TSA PreCheck Touchless ID and Boarding Gates). The routine use of facial recognition in

aviation raises questions of individual and collective privacy and the normalization of surveillance infrastructure, data security, possible scope creep or sharing across agencies, and negative impact on travelers through false positives or negatives, particularly with respect to demographic differences in accuracy and error rates.

The report draws upon the lived experiences of hundreds of travelers across the United States who completed a survey known as the TSA Scorecard prepared by AJL, as well as a recently issued government report assessing the TSA's use of facial recognition, AJL's prior research and campaigns, and research and advocacy efforts by civil society and policy makers.

AJL found concerning gaps in the facial recognition program's transparency, travelers' ability to consent, and the treatment of travelers by TSA officers. Our report finds that many travelers across 91 airports who completed the surveys experienced the program as mandatory even though TSA presents it as voluntary; travelers are not consistently given the opportunity to opt out; and some travelers face hostile treatment by TSA officers when attempting to opt out.

In the survey conducted by AJL of hundreds of travelers, 99 percent indicated that they were not told verbally by TSA officers of the opportunity to opt out. Nearly three out of four respondents indicated that they did not receive a notice about the use of face scans.

AJL's recommendations focus on preserving freedom and privacy, promoting informed public decision making, and preventing and redressing disrespectful treatment.

In particular, AJL recommends a halt of the TSA's use of facial recognition to allow for public deliberation and to address the concerns raised by the traveling public, civil society organizations, bipartisan elected officials, and the government's own Privacy and Civil Liberties Oversight Board.

COMPLY TO FLY? FINDINGS

March 2024 - June 2025
Timeline of collection for operational program findings

Scorecards

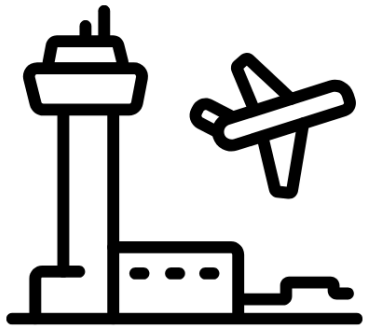
420

Verified scorecards submitted by travelers

Airports

91

Domestic airports visited by travelers in the U.S.



Transparency Gaps

56%

DID NOT SEE OPT OUT INFO
on airport signage about TSA facial recognition

74%

DID NOT RECEIVE NOTICE
about use of TSA facial recognition

Consent Gaps

99%

WERE NOT VERBALLY TOLD OF RIGHT TO OPT OUT BY TSA OFFICER

51%

UNABLE OR TOO UNCOMFORTABLE TO ACT ON RIGHT TO OPT OUT OF TSA FACE SCANS

Did not know opt out was an option, were scanned before they could opt out, did not feel comfortable opting out, fear that opting out could lead to negative consequences and/or requested to opt out but were denied

Overall Concerns

87%

Travelers from the operational period who shared concerns about the program including minors being scanned, surveillance risks, and more

Data Handling

33%

Travelers who shared concerns about data handlings.

Includes data sharing, lack of data privacy, distrust over deletion of face data, and more

Negative Treatment

Travelers who reported negative treatment by TSA officers, **out of the 192 travelers who shared their treatment by TSA.**

67%

Includes verbal abuse, public shaming, and perceived additional scrutiny

*!#@

AJL.ORG/FLYREPORT

INTRODUCTION

The **Comply to Fly?** report by the Algorithmic Justice League focuses on the facial recognition program operated by the Transportation Security Administration (TSA) at U.S. airports. While originally described as a "pilot" or "proof of concept" by TSA, the program has steadily expanded to over 250 airports as of May 2025 [1].

This report draws upon hundreds of travelers' lived experiences, through AJL's Freedom Flyers Campaign [2]. Launched in 2023 as part of its goal to provide everyday people with a means to share experience with AI, the Freedom Flyers Campaign has sought to gather feedback on people's lived experiences with the facial recognition program conducted at TSA checkpoints. Through this participatory data gathering initiative, AJL asked travelers to submit a TSA scorecard documenting their experiences, informed travelers of the right to opt out, and invited them to share their experiences on social media and with others in their communities [3].

The survey was complemented by social media campaigns aimed to raise awareness

of travelers' right to opt out, written testimony to the U.S. Commission on Civil Rights, as well as a Freedom Flyers Summit to protect biometric rights [4], [5].

The timeliness of this report is underscored by the release in May 2025 of a staff report by the Privacy and Civil Liberties Oversight Board (PCLOB) on the use of facial recognition technology by TSA, as well as bipartisan interest in understanding, assessing, and overseeing this program [1].

The AJL report complements the PCLOB report by providing vital missing information: the perspectives and lived experiences of hundreds of travelers across the U.S. as they navigated TSA's experimental facial recognition program.

The audience for our report is the traveling public, civil society organizations, elected officials, and policy makers committed to preserving privacy and civil liberties as an essential part of U.S. democracy. Additionally, given that governments around the world from established democracies to emerging economies embrace the use of biometrics in accessing government services and benefits, particularly border control, the report's findings and recommendations have global relevance.

OBJECTIVES

The objectives of AJL's report are to:

- Capture travelers' lived experiences with the facial recognition program conducted at TSA checkpoints around the United States.
- Document patterns of concern from the traveling public about the TSA program, the treatment of travelers, and the transparency about the voluntary nature of the program.
- Create greater public awareness of the ethical and rights implications of the use of facial recognition in aviation security and government services, and the tradeoffs and considerations.
- Provide recommendations for the traveling public, policy makers, elected officials, and government agencies to strengthen transparency and oversight, and address consent and traveler treatment.

The release of a recent report by the Privacy and Civil Liberties Oversight Board (PCLOB)—based upon an oversight project on facial recognition and other biometric technologies in aviation security launched in 2019—underscores the timeliness and importance of assessing this program [1]. Even though TSA's mechanisms to submit complaints or grievances do not include the specific use of FRT as a category of concern, the PCLOB report identifies **97 complaints** that referenced the use of FRT that were filed by travelers with TSA in the period May 2023 to February 2024 [1, pp. 4, 82].

AJL's approach of centering the experiences of travelers across the U.S. fills a unique gap, providing hundreds of traveler stories and data points from across the country. Our overarching objective is to center the lived experiences and perspectives of the public and ensure that society preserves individual and collective privacy and civil liberties in an era of increased AI-powered biometric technologies that enable the creation of mass surveillance infrastructure

METHODOLOGY

Launched in 2023 by the Algorithmic Justice League, the Freedom Flyers Project [2] assesses how traveler experiences compare to the stated design of the experimental facial recognition program operated by TSA. Hundreds of travelers shared their experiences with TSA through a survey that is available on the AJL website, shared on social media, and circulated through email and newsletters to a wide range of audiences. The survey included both structured input as well as open-ended text boxes, which were manually tagged[1] to allow for quantitative analysis.

[1] See Appendix E for a full list of tags.

In 2024, AJL shared preliminary findings with the U.S. Commission on Civil Rights [4]. AJL has held public events including the inaugural Freedom Flyers Summit [5] to raise awareness on this issue, and has met with DHS and TSA representatives to raise patterns of concerns voiced by travelers through AJL's Freedom Flyers Project. During RightsCon 2025, AJL shared a preview of a selection of 2024 scorecard submissions [6]. Through these avenues, AJL continues to highlight the ways in which the opt out nature of the program and even the right to opt out are not clearly understood by the public.

This report draws upon the hundreds of TSA scorecards submitted to AJL by travelers across 91 airports in the U.S. regarding trips taken from March 2024 to June 2, 2025 (the period after which the TSA's facial recognition program was considered fully operational [1, p. 39]), the AJL testimony presented to the U.S. Commission on Civil Rights, the discussions at the Freedom Flyers Summit, and the May 2025 report issued by the Privacy and Civil Liberties Oversight Board [1], [3], [4], [5].

BACKGROUND AND CONTEXT

Created in the aftermath of the September 11, 2001 terrorist attacks, the Transportation Security Administration (TSA) was established by the Aviation and Transportation Security Act [7] to ensure the safety and security of transportation. While initially part of the Department of Transportation, TSA became part of the newly created Department of Homeland Security in 2003 [8]. The Patriot Act was also passed weeks after 9/11, expanding the surveillance capacity of the U.S. government [9].

The expansion of the U.S. government's surveillance infrastructure and reach was complemented by a global expansion, which has been met by increased attention of policy makers and civil society organizations to the potential for government overreach and the threat of data breaches. The EU AI Act, for example, prohibits the live use of general facial recognition in public spaces because they assess the technology to be discriminatory and invasive [10].

TSA began exploring the use of facial recognition technology at U.S. airports starting in 2017 [1]. The experimental application of this controversial biometric technology began a rollout of devices with facial recognition capabilities (Credential Authorization Devices or CAT) at security checkpoints in 2023 [1].

This use of facial recognition technologies in the airport is part of a broader trend of a wide range of biometric technologies being used in a variety of spaces, including sporting events and concerts, public housing entry systems, and even in schools and churches [11].

A group of U.S. Senators raised concerns around the use of facial recognition technology by the TSA in 2023, at a time when the technology was used in only 16 airports [12]. “Increasing biometric surveillance of Americans by the government represents a risk to civil liberties and privacy rights,” they wrote to the TSA Administrator [12]. “Thousands of people daily are encountering a decision to travel or safeguard their privacy- a decision that threatens our democracy” [12]. Yet, since that letter was sent, the TSA has expanded its use of facial recognition technology to more than 2,100 devices at more than 250 airports, with plans to expand to over 430 airports [1, p. 80]. Furthermore, TSA has indicated that facial recognition technology is likely here to stay [1, p. 41].

In 2024, a bipartisan group of U.S. Senators led by Sens. Jeff Merkley (D-OR), John Kennedy (R-LA), and Roger Marshall (R-KS) wrote, “This technology poses significant threats to our privacy and civil liberties, and Congress should prohibit TSA’s development and deployment of facial recognition tools until rigorous congressional oversight occurs” [13].

At the state and local levels, elected officials from states such as Maine to cities such as Boston and San Francisco have limited or banned the use of facial recognition technology, expressing concern about the potential for misuse and scope creep [14], [15], [16].

In May 2025, the U.S. Privacy and Civil Liberties Oversight Board (PCLOB) issued a staff report on the use of facial recognition technology by the TSA [1]. An independent agency within the Executive Branch established by the 9/11 Commission Act of

2007, PCLOB initiated an oversight project in 2019 on the use of facial recognition and biometric technologies in aviation security [1]. The PCLOB report provides an overview of the TSA program, highlights privacy and civil liberties risks, and shares recommendations for program improvement [1].

The PCLOB report highlights a range of issues and provides related recommendations with respect to program effectiveness and value, consequences of misidentification and demographic impacts, transparency and public notice, individual rights, data policy, and safeguards against expansion or misuse [1]. Key findings and recommendations from the PCLOB report reinforce AJL's own findings and recommendations from its survey data.

In addition to AJL, civil society groups such as Fight for the Future, the Electronic Frontier Foundation, the American Civil Liberties Union, and Electronic Privacy Information Center have also been tracking and advocating around the expansion of facial recognition and biometric technology by the TSA [17], [18], [19], [20]. Significant media coverage from the Washington Post to Fast Company has maintained awareness of this important public concern that affects millions of people's privacy and civil liberties [21], [22].

The expanding use of facial recognition technology by TSA (and other government agencies) raises significant ethical considerations and questions. The rights to privacy and autonomy in a liberal democracy such as the United States, combined with the implications of the proactive collection of biometric information from all travelers, many of whom have not committed a crime, require us to view this program through more than the twin lenses of enhanced security and efficiency.

The reality of data breaches,[2] the potential to combine data from different government agencies and companies to create comprehensive profiles of individuals, and the possibility that TSA could increase its retention period of travelers' digital images and sensitive biometric data, necessitate closer monitoring, oversight, and regulation

[2] See for example the 2015 cyber incident resulting in the loss of of sensitive data of over 21 million people, including 5.6 million sets of fingerprints held by the federal government [1], [23] and the 2019 cyber incident resulting in the loss of images of 184,000 travelers which had been captured during a facial recognition pilot by DHS [1], [24].

by Congress, as well as advocacy and awareness among civil society, the media, and the general public.

In the U.S., privacy law is in part based on court rulings which use a standard of "reasonable expectations of privacy" to interpret privacy rights.[3] Changing the overall expectations of privacy, through the expansion of facial recognition technology and other biometric technologies for millions of domestic travelers, could result in our unwitting acquiescence to living in a surveillance society.[4]

Unique considerations in the context of border control for refugees, asylum seekers, and stateless persons, as well as trans individuals require awareness that the impacts of facial recognition technology are not evenly felt across all individuals and communities. Non-citizens typically have fewer rights at border points than do U.S. citizens [26].

According to Tendayi Achiume, the former U.N. Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, "Executive and other branches of government retain expansive discretionary, unreviewable powers in the realm of border and immigration enforcement that are not subject to the typical substantive and procedural constraints, constitutionally and otherwise guaranteed to citizens" [27].

Traveling while trans also poses unique challenges for trans travelers, with facial recognition technology and photographs in IDs sometimes resulting in a mismatch, resulting in enhanced screening [28]. Fifty-nine percent (59%) of respondents in a 2022 U.S. Transgender Survey who had at least one ID said that none of their IDs listed the gender they wanted [29].

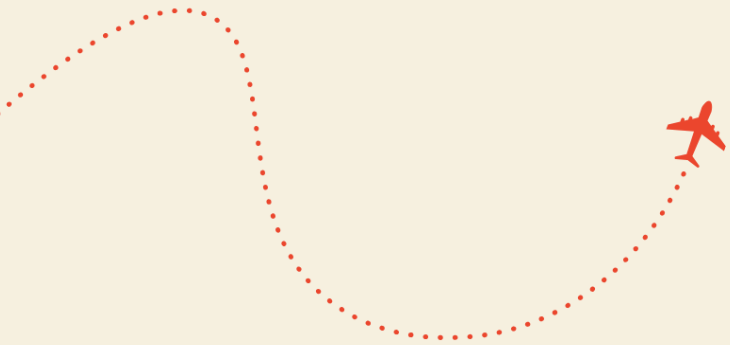
With high-profile cases of facial recognition technology implicated in the wrongful arrest of people of color [30], advocates and elected officials have raised concerns about demographic differentials and the potential for inaccuracy or bias in facial recognition and other biometric systems [12], [31], [32], [33].

With our faces as the "final frontier of privacy," [34] concerns raised by elected officials across party lines and across the

[3] In the 1967 case *Katz v United States* [25], the U.S. Supreme Court ruled that it is unconstitutional under the Fourth Amendment to conduct a search and seizure without a warrant anywhere that a person has a "reasonable expectation of privacy." The concurring opinion created a two-part test for determining this: (1) The individual has exhibited an actual expectation of privacy and (2) The expectation is one that society is prepared to recognize as reasonable. The "reasonable expectation of privacy" standard has evolved in subsequent court rulings.

[4] In other words, once the technology becomes familiar and feels normal in one setting (the airport), its introduction in new settings (such as entry to government buildings) may be less likely to be successfully challenged.

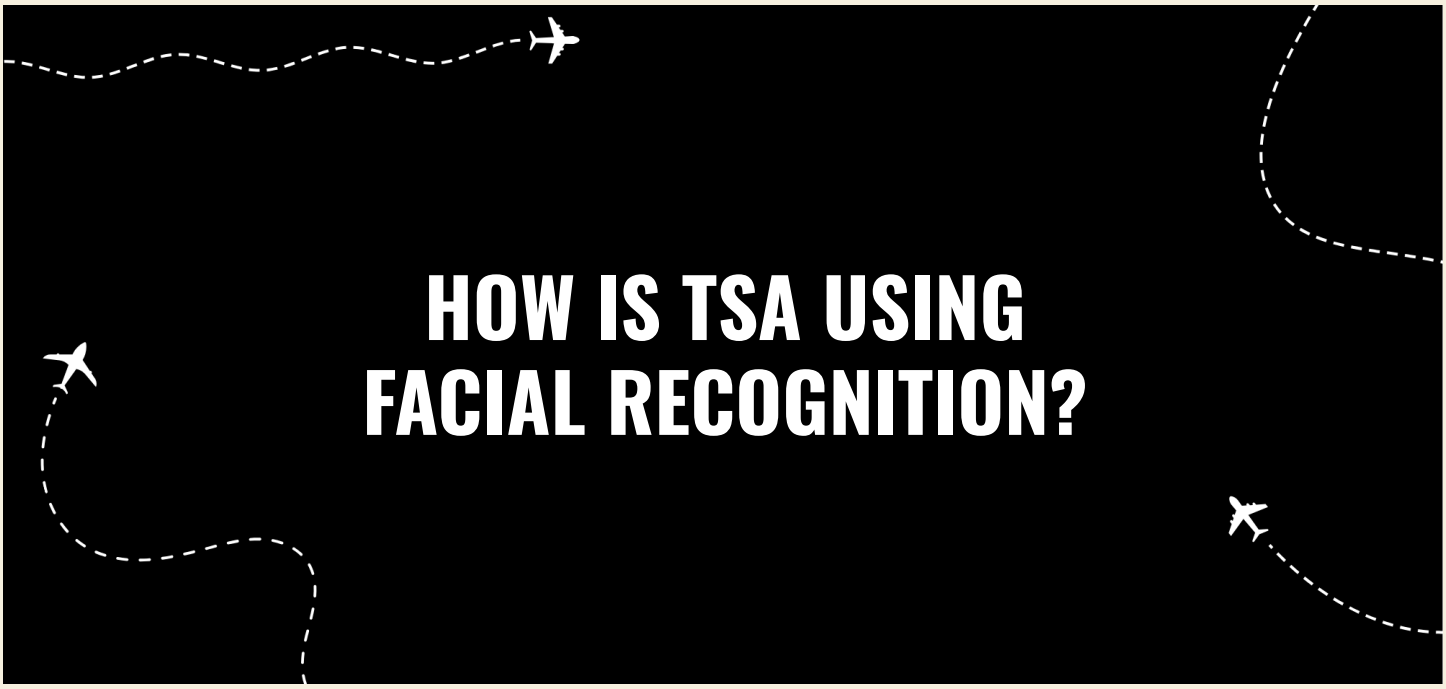
country, as well as by civil society organizations emphasize the potential for biometric data to be used across government agencies or retained and stored for longer periods of time. The claims of greater efficiency and safety have not been substantiated, with a bipartisan group of twelve senators, in a letter to the DHS Inspector General in November 2024, noting 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" [35].



Given that there are no statutes to prevent further expansion and the DHS directive related to the program's oversight was taken down from the DHS website in February 2025,[5] TSA needs to make a case for the program's value, effectiveness, and approach to protecting biometric and biographic data and individuals' civil liberties so that informed deliberation can occur on the future of the program.

Airport face scans are one component of a larger societal conversation on biometric rights and consent in the algorithmic age. AJL's aim is that public awareness, deliberation, and consent are seen as vital before the introduction and expansion of biometric technologies given the potential for government and corporate surveillance to fundamentally transform how we as individuals live healthy, safe, unexamined, and dignified lives.

[5] The PCLOB report notes that DHS Directive 026-11, "a set of rules governing the use of facial recognition and related technologies for all DHS components," was removed from the DHS website in February 2025, and DHS did not clarify whether the Directive still applies [1, pp. 22–23].



HOW IS TSA USING FACIAL RECOGNITION?

Public understanding of facial recognition is influenced by films like *Mission Impossible* or TV shows where law enforcement officials use security cameras to attempt to find an individual in a public space [36], [37]. Consumer products like iPhones have also increasingly exposed the public to the use of facial recognition to grant access to the use of consumer devices [38]. These examples show two distinct uses of facial recognition that are also now occurring in airports. Because there are different ways technology can be used to scan human faces, AJL uses the term facial recognition technologies (FRTs) [11].

FRTs encompass an entire suite of biometric face technologies, including those used for face detection, gender classification and age estimation, face identification (1:N), and face verification (1:1) [11]. Industry use of the term facial recognition often refers to the latter two (face identification and face verification).

The TSA uses terms like “biometric identification verification” on some signage to refer to its use of facial recognition [4]. The agency refers to machines that can be equipped to scan faces using Credential Authentication Technology 2 which is termed as a “CAT-2 unit” in agency

communications [1]. Travelers may find these terms confusing and not understand these TSA terms indicate the use of facial recognition.

To add clarity, this section outlines how two distinct types of facial recognition methods are used in U.S. airports by TSA.[6]

FACIAL VERIFICATION (1:1 MATCHING)

Used at TSA Security Checkpoints | Used in Consumer Devices like iPhones

Live Capture of Face Image	TSA officer initiates the device to take an image of the traveler.
Creation of Faceprint	The image is processed by AI to create a mathematical representation of the face called a faceprint or template. Like a fingerprint, a faceprint is thought to be a unique identifier of an individual.
Matching	The new faceprint is matched against an existing faceprint derived from the traveler's ID or Passport presented to the TSA officer.
Decision	If the faceprints are evaluated to be similar enough, the traveler is **verified**. If the faceprints are evaluated to be too dissimilar, the traveler is not verified and may be asked to try again.

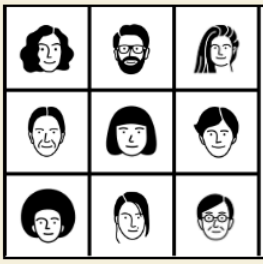
[6] Tables informed by the PLCOB Report [1] and adapted from AJL's Facial Recognition Technologies: A Primer [11] and the 2024 TSA Scorecard Preliminary Results presented at RightsCon 2025 [6].

FACIAL IDENTIFICATION (1:N MATCHING)

Used at TSA PreCheck Touchless ID | Can Be Used By Law Enforcement for Surveillance

Live Face Image Capture	The image is taken and sent to a cloud-based program run by CBP called “Traveler Verification Service.”
Creation of Faceprint	The image is processed by AI to create a mathematical representation of the face called a faceprint or template. Like a fingerprint, a faceprint is thought to be a unique identifier of an individual.
Matching	This faceprint is compared to a database of existing faceprints – derived from a database/gallery of DHS-held photos of everyone who is scheduled to be traveling through the airport on the same day.
Decision	If the traveler’s faceprint is evaluated to be similar enough to a faceprint in the DHS gallery, the traveler is **identified** in the gallery. If the faceprints are evaluated to be too dissimilar, the traveler is not identified in the gallery, and may be asked to try again. The traveler could also be matched to someone else and permitted access. The larger the gallery, the higher the possibility of being matched to someone else.
Enrollment	For there to be other faces to be compared to, there must be an enrollment process where a database of faces is created. For TSA, these enrollment photos can come from passport images or identification photos submitted when enrolling in trusted traveler programs like PreCheck, and photos taken by DHS in past border crossings.

FACIAL RECOGNITION FOR TSA PRECHECK TOUCHLESS ID



GALLERY

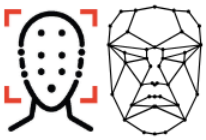
Before the system is used, a gallery is created by uploading images of each traveler to be recognized and computing a faceprint from each image.

Source: American Airlines

This image shows the process of using facial recognition for TSA PreCheck Touchless ID

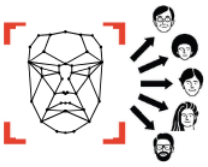
1 IMAGE CAPTURE

To proceed past the TSA checkpoint, a person poses for a picture. The captured photo is the live image.



2 FACEPRINT CREATION

The system converts the live image of the person into a faceprint, a digital representation of the face.



3 COMPARISON TO GALLERY

The faceprint of the person is compared against the faceprints of travelers in the gallery.

4 ACCESS DECISION

If the faceprint matches a traveler, the person is allowed to pass the checkpoint. If there is no match, a manual check may be required.

[Figure A] - Facial Recognition for TSA PreCheck Touchless ID. *Photo source: [39]*

The performance of FRTs has received considerable attention with ongoing academic and government studies that show different algorithms perform differently on different faces on the basis of age, gender, race, and their intersections [40], [41], [42], [43]. These differences are typically referred to in government reports as “demographic differentials” and in academic studies as “algorithmic bias.”

For the traveling public, it is important to understand that it is not enough to know the overall accuracy of a given system. Anyone evaluating these systems needs to know the

errors these systems can make and the consequences of the errors.

Two important concepts in assessing the accuracy of a deployed version of facial recognition technology are false negatives and false positives. These two types of errors have different consequences for travelers depending on the type of matching used.

A false negative means that a traveler is incorrectly flagged as not matching their credentials. This error might result in the TSA officer requiring rescanning of documents, additional screening of the traveler, manual verification of identity, and in the worst case, the denial of entry to the boarding area. Such errors not only delay other travelers in line, but they can cost the traveler time and money. In government studies, false negative rates have been shown to vary by race, and reports from trans travelers indicate they might face additional barriers [44], [45].

A false positive means a traveler's face is matched to the face of someone else. This can be thought of as a case of mistaken identity. False positives can result in an imposter gaining access to the boarding area. In the case of verification (1:1 matching) the traveler is checked against the credentials they provide. In the case of identification (1:N matching), the traveler is being cross checked against the faces of travelers in the gallery of potential matches, which could include all expected travelers for the day. If the gallery in the future includes a watch list of suspects or a "no fly" list, a false positive might result in the traveler being falsely matched with a suspect **or individual who is not permitted to board an aircraft** [1].

Being flagged as matching a suspect can result not just in missing a flight but also public humiliation, bodily harm, and in the worst case escalation to detention, false arrest, or fatal encounter with law enforcement.
The larger the gallery size, the greater the likelihood of a false positive [1, p. 18].The risk of misidentification and follow-on consequences make the stakes of deploying 1:N matching in airports even higher than 1:1 matching.

Despite advancements in technology over the past few years, false positives and negatives can result in minor delays at best and more consequential outcomes at worst.

DEMOGRAPHIC DIFFERENCES IN ERROR RATES PERSIST

The landmark 2019 NIST Demographics study [43] documented demographic differentials as high as factors of 100 more false positives between countries of origin [43]. These results led to widespread media coverage on the discrimination risks of facial recognition and coincided with the same year PCLOB began assessing TSA's use of facial recognition. Since then, ongoing evaluations of facial recognition algorithms show that despite overall accuracy gains, demographic differentials persist, especially for Black individuals, women, and older individuals [46].

PCLOB's report visits some of the performance metrics of the facial recognition software used by the TSA.

According to the government report, in 2024 the algorithm used for 1:1 matching had 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)" [1, p. 69].

For false negatives, the "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" [1, p. 69].

SUMMARY OF FINDINGS

When reviewing survey data, we found concerning and consistent gaps in the program's transparency, travelers' ability to consent, and the treatment of travelers by TSA officers. These gaps will be explored in depth in this Section.

A. DATA BREADTH & DEMOGRAPHICS

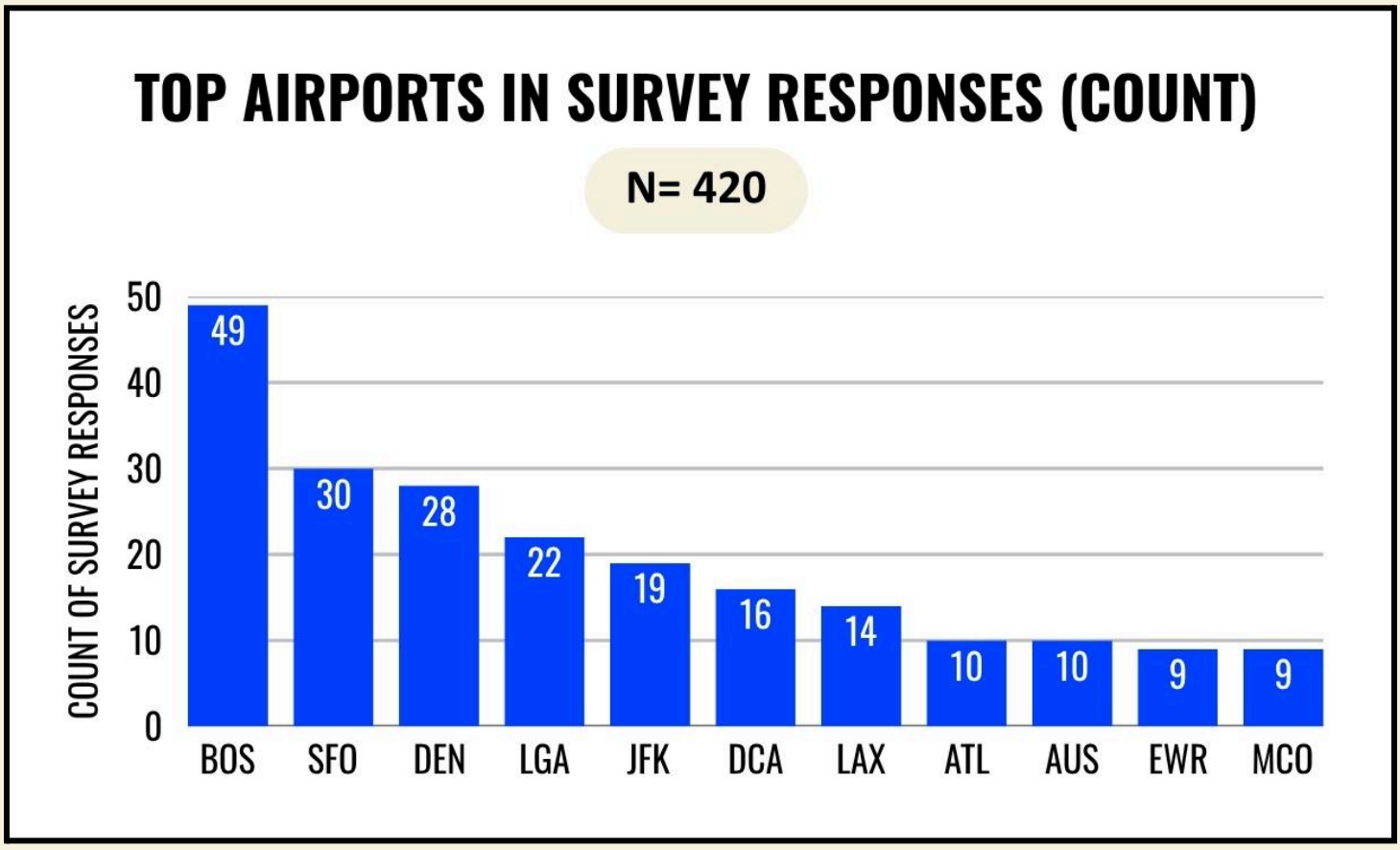
In total, we received 864 survey responses between 2023 and June 2, 2025. For this report we focused our analysis on data pertaining to flights on or after March 1, 2024, since this is when TSA considered their facial recognition program to be fully operational [1, p. 39]—earlier survey responses may have indicated problems that were subsequently solved by TSA during their testing phase. We also look at broad trends in traveler experience throughout the full survey period, delimiting between the pre-operational period and operational period. Some survey responses contained information about experiences with Customs and Border Protection (CBP) at international border crossings or experiences with the use of facial identification by airlines at boarding gates. These survey responses were excluded from the analyses. After filtering, we

examined 420 survey responses during the operational period. Unless otherwise indicated, analysis in this section will be based on those 420 responses.

The TSA identified 97 complaints about the facial recognition program between May 2023 and February 2024, a relatively small number compared to the 2,000 daily reports the TSA receives [1, p. 82]. The more than 800 survey responses we received highlights that the small number of complaints the TSA received was not indicative of a lack of travelers experiencing issues or having concerns with the program, but rather, as the PCLOB report states, an inability for travelers to appropriately report their concerns [1, p. 82].

OPERATIONAL EXPERIENCES

The survey results included **91** airports, with the highest number of responses from Boston Logan International Airport, San Francisco International Airport, Denver International Airport, LaGuardia Airport, John F. Kennedy International Airport, and Ronald Reagan Washington National Airport.



[Figure B] - Airports Most Frequently Represented in the Survey Data

Starting in 2024, survey respondents could share demographic information including age, racial identity, and gender identity. Demographic data was not visible while manually labeling the data. We received responses from travelers from respondents from all age groups between 14-16 through 75+. 70% of respondents who shared their age were between the ages of 25 and 56.

Respondents shared gender identities including cisgender and transgender women and men, nonbinary, and other. Respondents' shared racial identities spanned 9 U.S. Census racial categories: White, Black or African American, Asian, Hispanic or Latino, Multiracial and/or Multiethnic, American Indian or Alaska Native, Native Hawaiian or Pacific Islander, and Some Other Race.

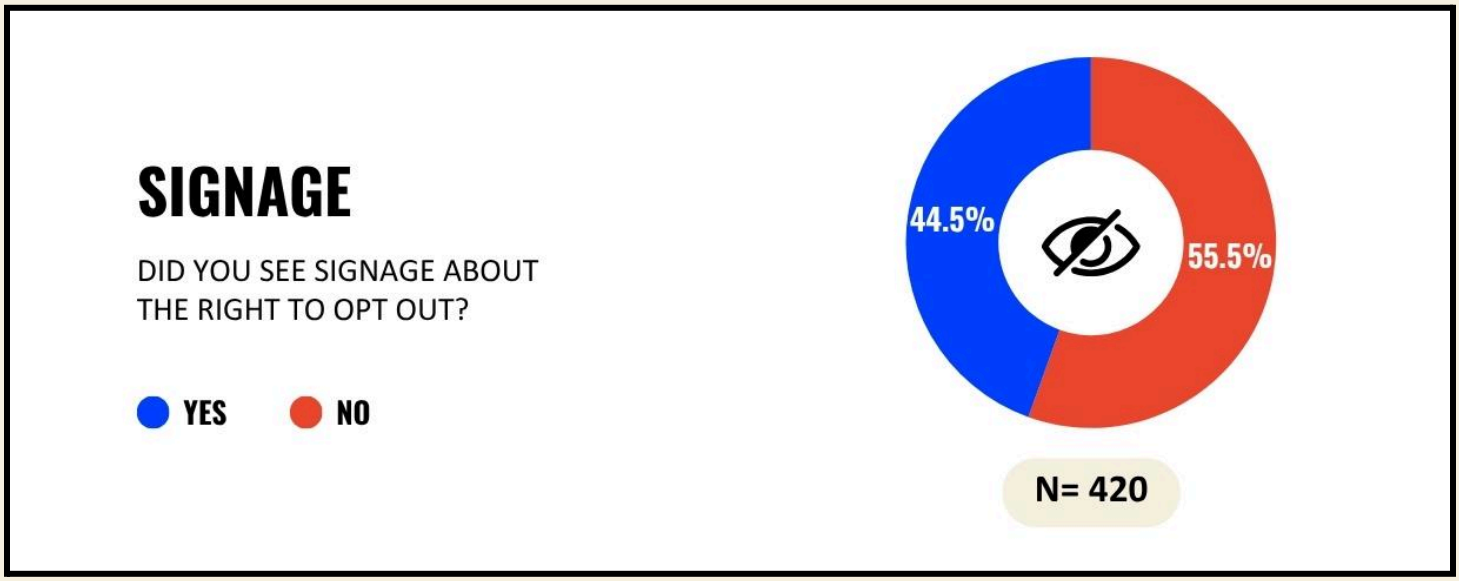
We found that all demographic groups experienced concerns and instances of negative treatment. Deeper analysis of demographic differentials warrants future study.

B. PROGRAM TRANSPARENCY

We found that current TSA efforts to inform travelers about the use of facial recognition are not reaching all domestic airport travelers: survey respondents reported missing signage, not receiving notice about the program, being concerned about data handling, being confused about the process, and having concerns around technical accuracy and bias and discrimination.

SIGNAGE

Travelers consistently missed seeing signage informing them about the Facial Recognition program, and their right to opt out.

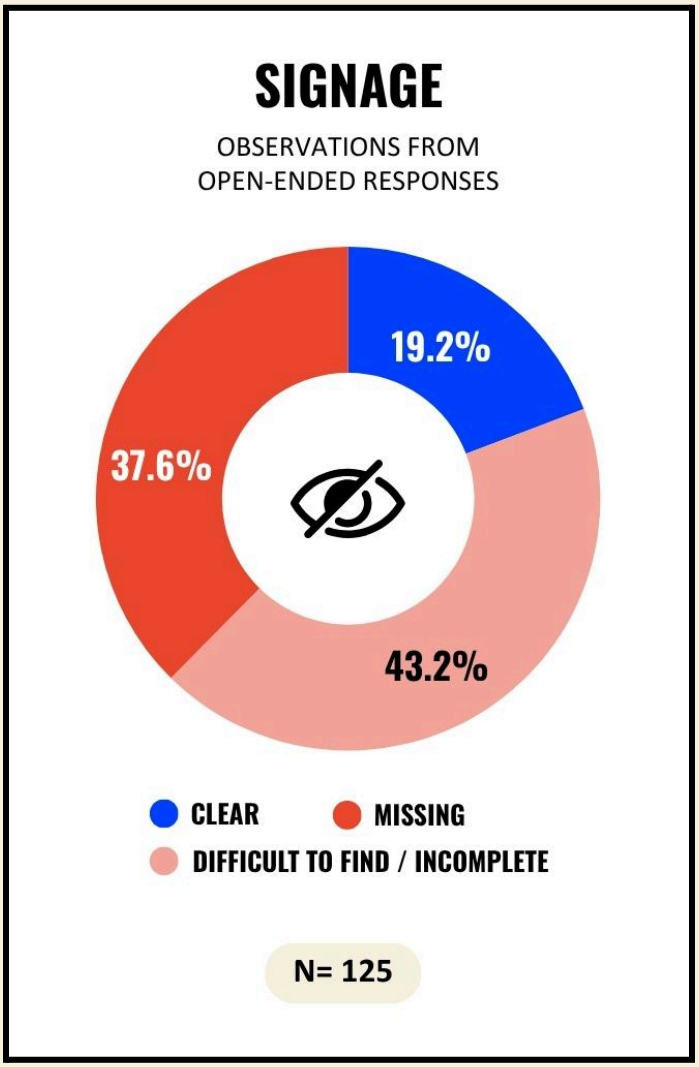


[Figure C] - Proportion of Respondents Who Saw Signage About Opting Out of Facial Recognition

55.5% of respondents (233) reported that they did not see signage about the right to opt out, and 44.5% of respondents (187) reported that they did.

Among 125 respondents who mentioned signage in their responses to open-ended questions, only 19.2% (24) mentioned seeing clear signage about the program. 33.6% (42) indicated that they did see signage, but doubted that other travelers would have been likely to see it. 14.4% (18) noted that they did see signage, but it was incomplete. For instance, it was missing information on whether one could opt out, how to opt out, or contained information that was not helpful, such as links for more information that didn't lead to real webpages. 37.6% (47) indicated that signage about the program was completely missing– either they didn't notice it or in some cases verified that there was no signage by enlisting the help of TSA officers to help look for the signage.

Signage Tags	Count
Signage Clear	24
Signage Difficult to Find (42) and/or Incomplete (18)	54
Signage Missing	47

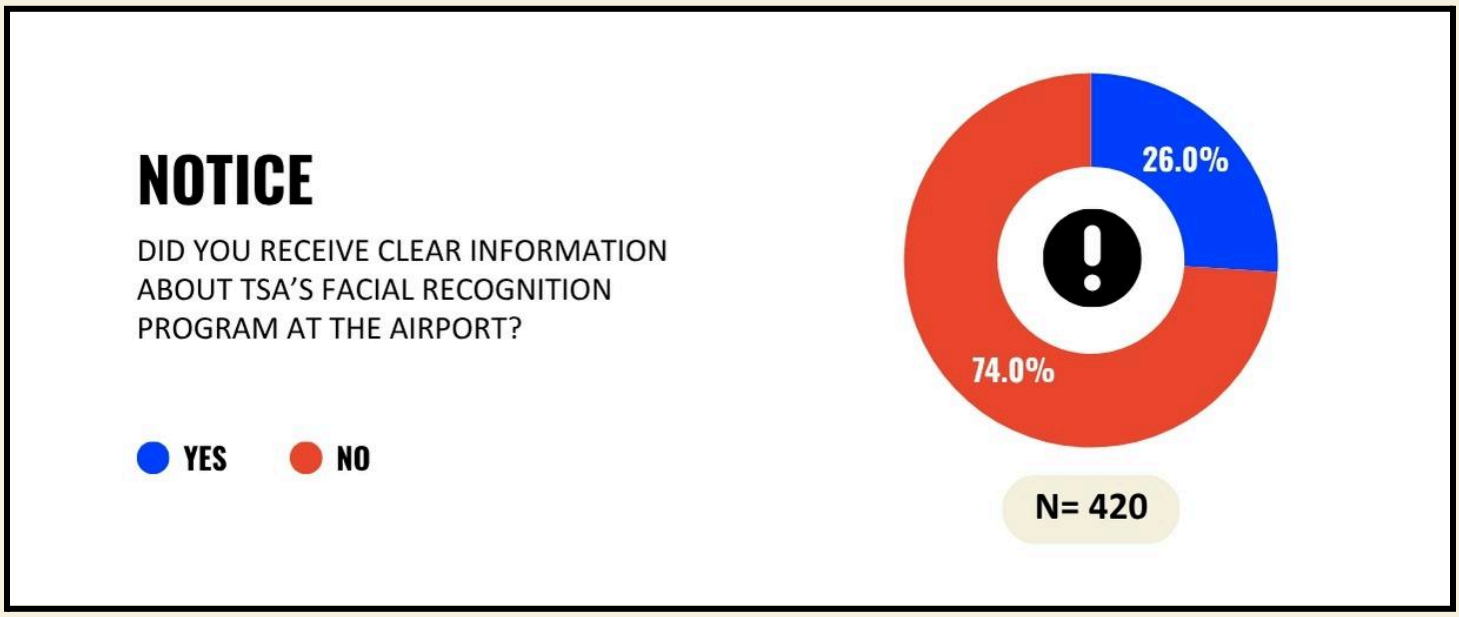


[Figure D] - Proportion of Respondents' Observations of t Facial Recognition Signage

NOTICE

Survey responses suggest that signage, even when visible, does not provide adequate notice to travelers: While 44.5% of all respondents (187) saw signage about the right to opt out, only 26% (109) said that they received clear information about TSA's facial recognition program at the airport. 74% of all respondents (311) indicated that they did not receive clear information about the program.

Among the 187 respondents who did see signage about the right to opt out, 48.1% (90) answered that they did not receive clear information about the program.



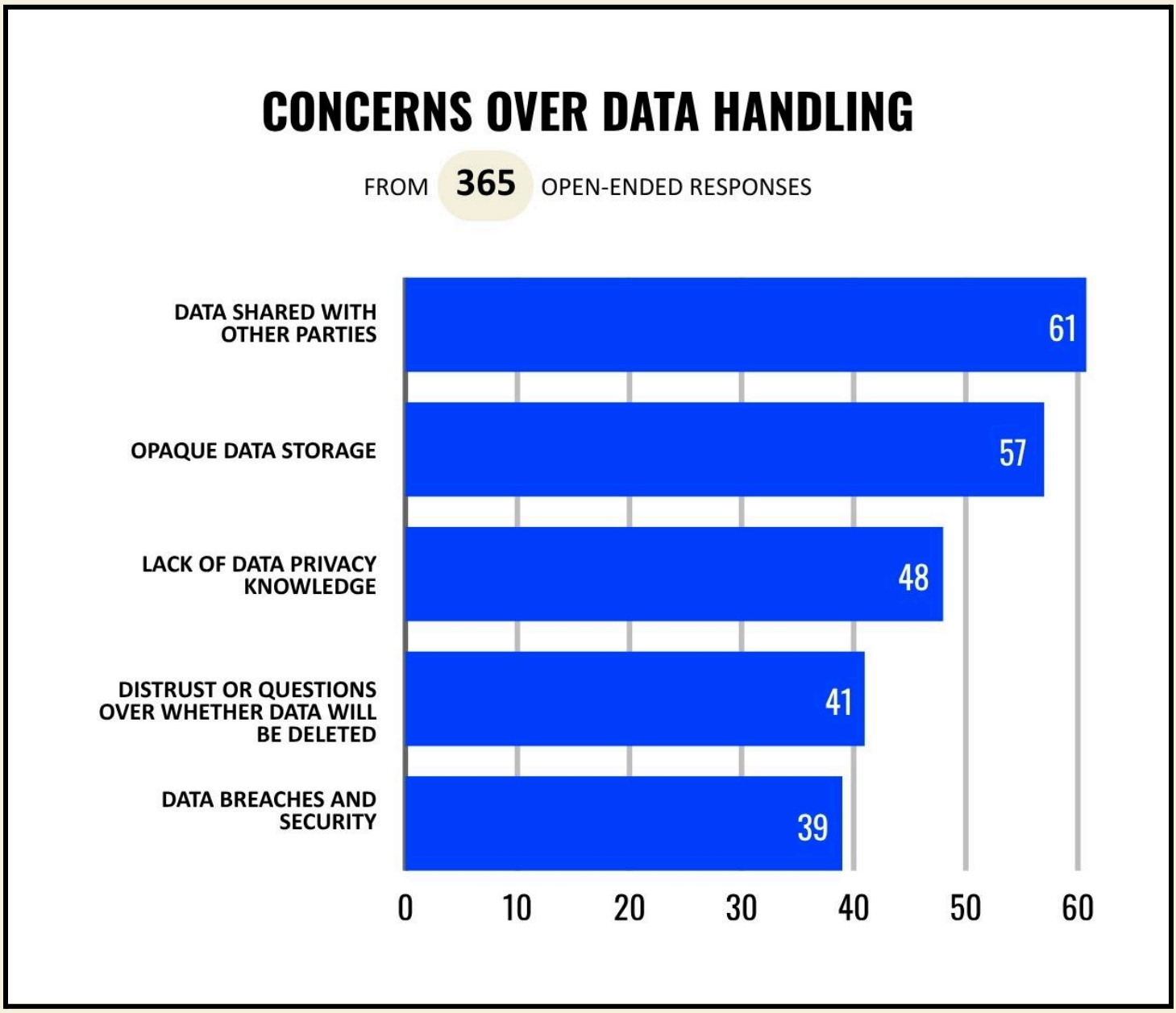
[Figure E] - Proportion of Respondents Who Received Information about Facial Recognition

DATA & PRIVACY PRACTICES

Travelers expressed concerns about data practices and privacy, indicating a lack both of transparency and trust in these practices.

48% (202) of respondents had at least one concern about general privacy and/or data handling practices. 32.9% (138) of respondents specifically shared concerns around data handling practices:

- 14.5% (61) had questions over whether facial data would be shared with other parties, including being sold to data brokers or shared with other government agencies.
- 13.6% (57) had concerns and questions over how and where the data is stored.
- 11.4 % (48) indicated an overall lack of data privacy knowledge.
- 9.8% (41) distrusted or questioned whether their data will truly be deleted within the timeframe TSA indicates.
- 9.3% (39) had concerns over data breaches and identity theft.



[Figure F] - Forms of Concerns Regarding Data Handling

SYSTEM ACCURACY AND DISCRIMINATION

Respondents also expressed concerns about the technical accuracy of the facial recognition systems as well as the possibility for bias and discrimination in open-ended responses. 39 respondents brought up concerns over biased and discriminatory systems, and 38 respondents brought up concerns over the technical accuracy of the systems. This included concerns over systems being less accurate for older individuals, darker skinned individuals, and trans or

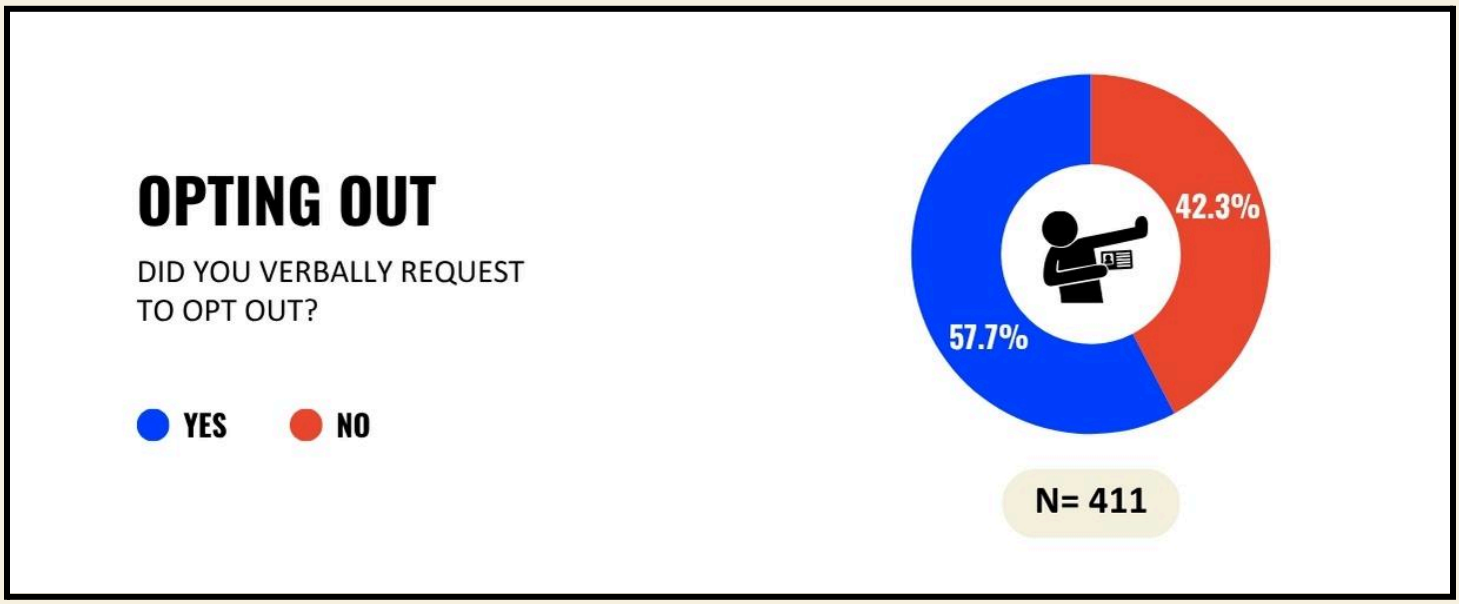
nonbinary individuals, and disparate treatment and discrimination that could occur based on false negatives.

> “I'm concerned about the way that my facial recognition may be shared with other agencies, contractors, etc. without my knowledge. I'm concerned about that ability of my facial recognition data to be improperly matched to someone else's identity, or my facial recognition data being matched with their data, given the well-documented inaccuracies of the technology being used with people of color.”
>
> ***Orlando International Airport, June 2024***

C. CONSENT

Survey responses indicate barriers to travelers’ ability to give informed consent to the program. For informed consent, travelers must know about the program and be given the opportunity to indicate consent.

411 travelers indicated that they either verbally requested or did not verbally request to opt out of the program. The remaining 9 travelers either did not respond to this question, or selected “Unclear” or “Other.”

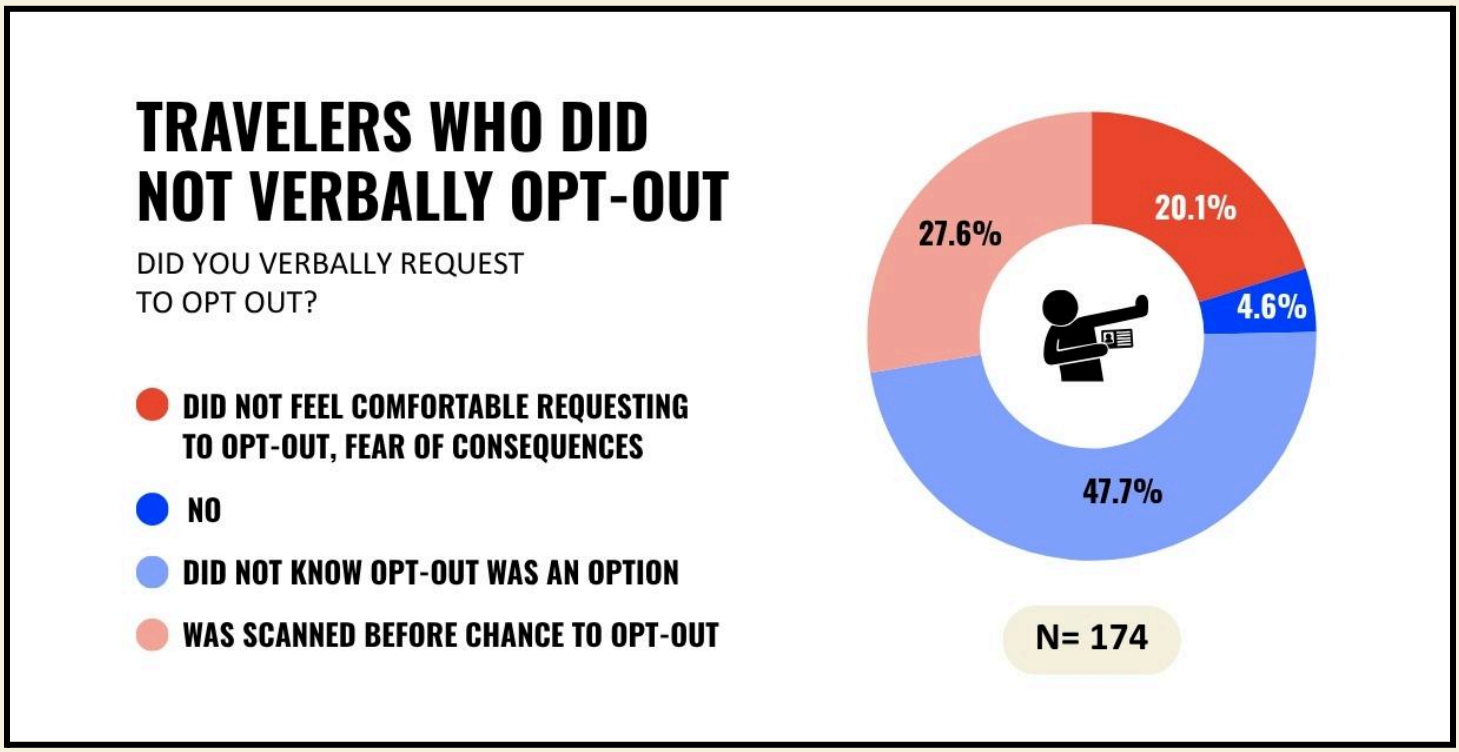


[Figure G] - Proportion of Respondents Who Verbally Requested to Opt Out

Out of the 411 that indicated whether or not they verbally requested to opt out, 57.5% (237) travelers indicated that they did request to opt out of TSA's facial recognition program. Of these 237, 82.3% (195) of travelers indicated that they were successful in opting out, while 12.2% (29) of respondents were unsuccessful in opting out.

42.5% (174) did not verbally opt out, but this did not necessarily signify an intention to opt in to the program. Out of these 174 respondents:

- 47.7% (83) answered that they did not know opt-out was an option.
- 27.6% (48) answered that they were scanned before they had a chance to opt out.
- 20.1% (35) answered that they "did not feel comfortable requesting to opt out; fear of consequences."
- Only 4.6% (8) chose "No" to indicate that they did not request to opt out.



[Figure H] - Answers from Respondents Who Did Not Verbally Request to Opt Out

Traveler's open-ended responses provided more information. Taking into account responses from open-ended responses as well as the travelers' responses to whether they verbally requested to opt out, out of 420 responses:

- 95 respondents noted being unaware that they could opt out.
- 82 respondents (including both those who did request to opt out and those who did not) reported being scanned before they had a chance to opt out of facial recognition.
- 49 respondents noted fears or discomfort about opting out, some fearing negative consequences for requesting to opt out.
- 56 respondents noted that they requested to opt out and were coerced or discouraged by the TSA officer.
- 36 respondents noted that they requested to opt out but their request was ignored or refused by the TSA officer.
- 29 respondents noted that they were told by TSA officers that it was "too late" to opt out.

23 respondents reported being told false information by TSA officers. This information was of varying severity and included:

- That the program was mandatory or would soon become mandatory
- That travelers would be “put on a list” for opting out
- That the police would be called

Respondents had concerns around consent:

- Out of the 365 respondents who shared open-ended concerns, 34.2% (125) wrote about the lack of informed consent.
- Some respondents (10) noted that cameras were pointed towards the line, meaning that they were unable to fully opt out of the program, since their faces were captured in other travelers’ photos.
- A few respondents (4) additionally noted that they were unable to fully opt out of having their biometric data scanned into the program, since their ID photos (containing biometric data) are still scanned during the manual verification process.

CONFUSION OVER PROCESS

The survey results also indicated that travelers were sometimes left confused about whether or not they were scanned, and when they were scanned, about whether or not facial recognition technology worked for them. This indicates gaps in both process transparency and informed consent.

- Among 237 travelers who requested to opt out, 13 travelers (5.5%) were unclear on whether their opt-out was successful or not.
- Out of 196 respondents who indicated that they may have been scanned, 65 (33.2%) indicated that they were unsure whether the technology worked.

SCANNING OF MINORS WITHOUT PERMISSION

A few respondents described concern over children being scanned without consent of their guardians. One traveler shared:

“The only reason I was able to opt out of facial recognition is because my partner was aware of it beforehand. We were struggling to see any signage that informed us of our right to opt out. There was one small sign on the side of the screen not directly visible to travelers unless pointed out.

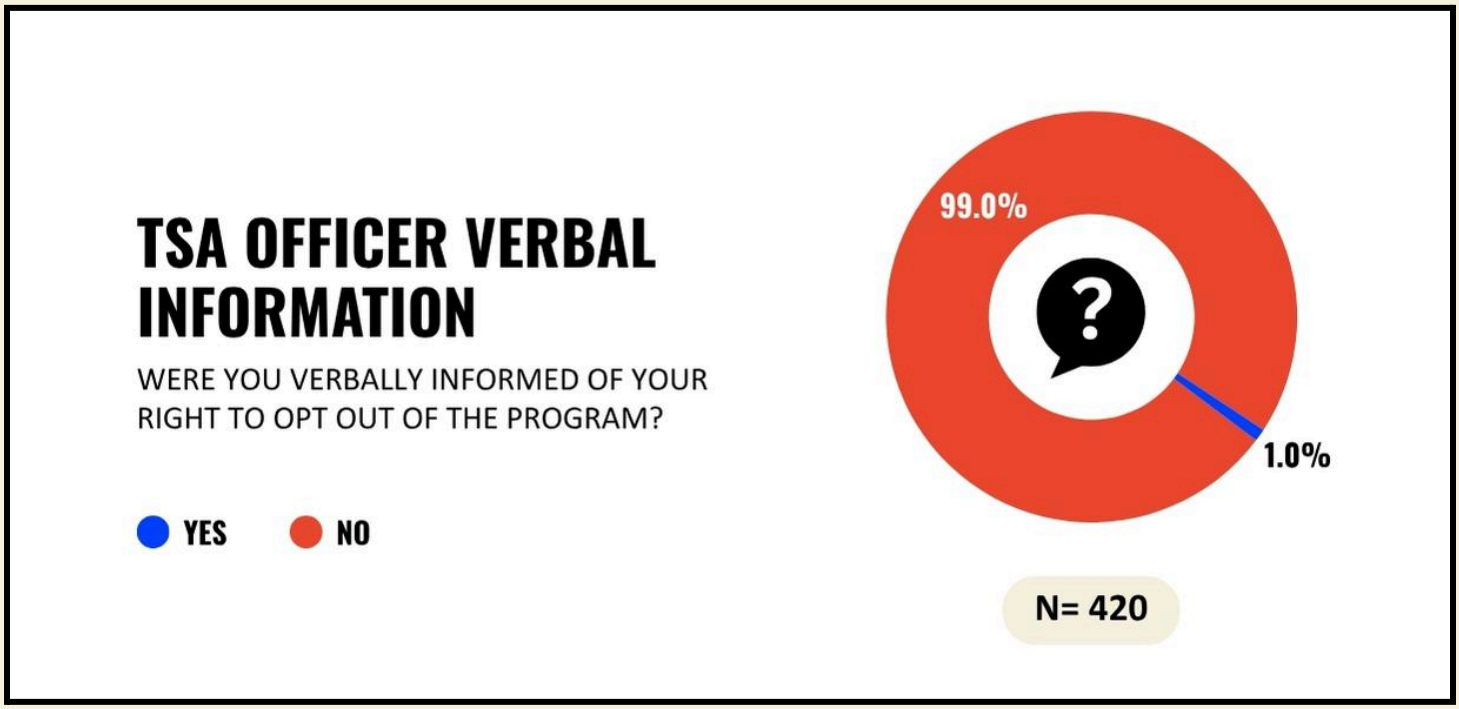
All travelers ahead of us were not informed of their right, and TSA was very quick to push them through to the scanner before they had a chance to see the signage. We saw moms struggling with their kids being pushed to the scanner without any opt out options being presented to them.

There were dozens of screens all around the TSA line that displayed everything except the opt out information and instead the opt out information was printed on a measly letter size paper only readable right in front of the scanner.”

San Francisco International Airport, July 2024

NO VERBAL ASK FOR CONSENT

In total, 99% of travelers were not asked for consent. Only 4 travelers (1%) indicated TSA officers seeking verbal consent to the program. However, in one of these instances, the traveler shared that after the officer asked for consent (and the traveler declined), the officer took a photo of the traveler's minor child without the guardian's consent.



[Figure I] - Proportion of Respondents Verbally Informed of Their Right to Opt Out

TIME SAVINGS AND EFFICIENCY

Travelers' open-ended responses revealed several aspects of perceptions around time-savings and efficiency of the program:

- 14 travelers expressed concerns that the facial recognition program increased verification time for passengers who opt out.
- 1 traveler, meanwhile, suggested that the facial recognition program resulted in faster verification time.

30 travelers mentioned time pressures—concerns about missing their flight or the length of the security line—as factors in their experiences. In particular, some of these travelers would have preferred to opt out, but were concerned that opting out would prevent them from reaching their flight in time.

27 travelers described being set aside for extra manual screening after opting out, an experience which increased their time through security. In one case, this extra time contributed towards a traveler missing their flight.

One traveler describes their experience of being set aside for manual screening:

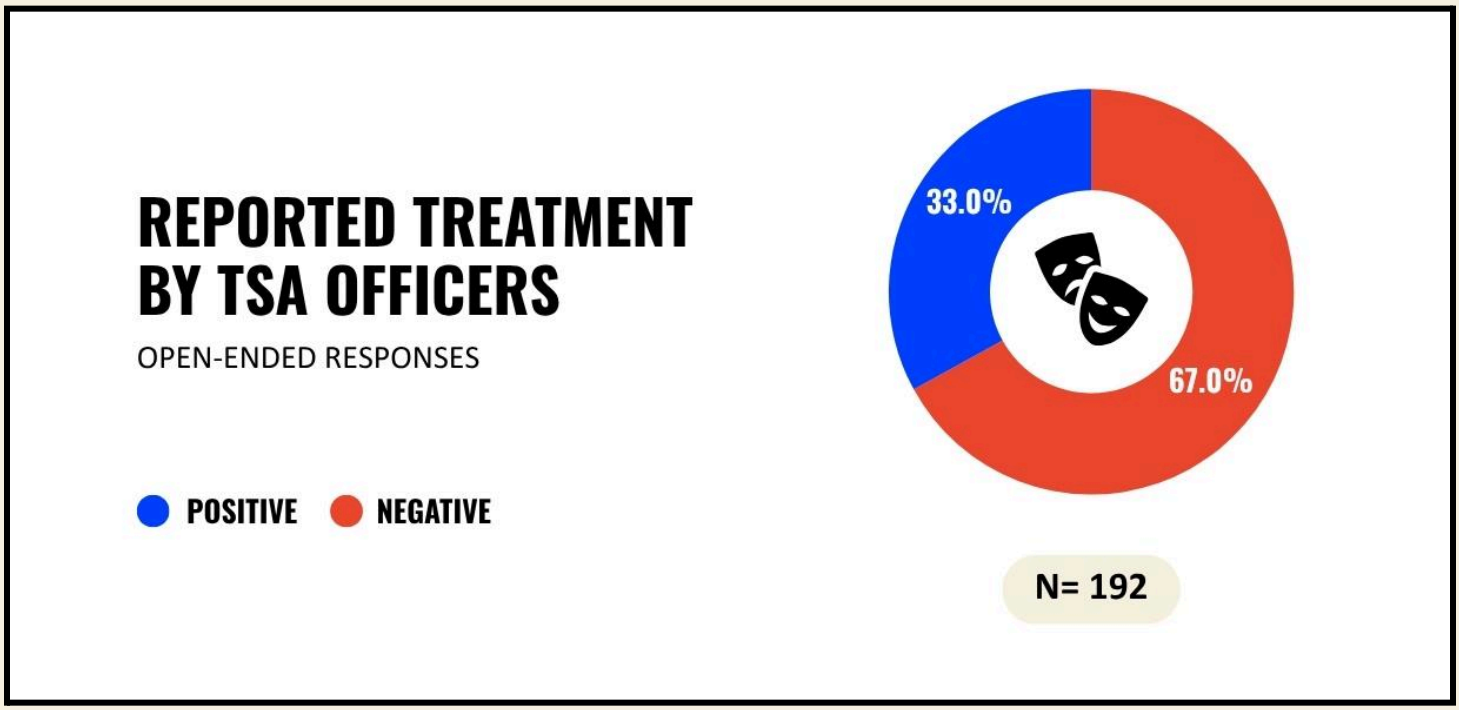
> “[W]hile passing through security … I requested my usual photo opt-out. This time, the TSA agent made quite a scene: she closed off her lane with a divider rope, took my ID and boarding pass to another lane, and left me waiting for five minutes. When she returned, she sat down and spent another five minutes scrutinizing my ID and boarding pass. Concerned, I asked if there was a problem.
>
> She replied, ‘No, I just have to verify everything manually; you should consider just allowing the photo next time.’ Finally, she handed my ID and boarding pass back and cleared me to proceed. The entire episode felt deliberate and intimidating.”
>
> ***Harry Reid International Airport, March 2025***

However, opting out need not take long nor be burdensome:

> “Thanks to being educated by [AJL] [...] I found out (for the first time) that the facial recognition scan is optional. When I got to the Las Vegas airport I simply walked up to TSA, handed the officer my license and when he asked me to stand in front of the photo scanner I said "I think that is optional. I would like to opt out please."
>
> He said "That's fine, you just have to tell me." He took my license after I scanned it in the machine and checked it and let me pass. (I stood to the side of the photo machine.) It was simple and easy. I was nervous about what would happen but in this case TSA was easy about it.”
>
> ***Mccarran International Airport. March 2025***

D. TREATMENT

Out of the 192 travelers who described how they were treated by TSA officers in open-ended responses, 67% (130) reported negative treatment, and 33% (64) reported being treated with respectful speech or body language, in line with TSA personnel guidelines to treat travelers with dignity and respect. (Note that two passengers described both negative and positive treatment by different TSA officers, so these responses are counted in both categories.)



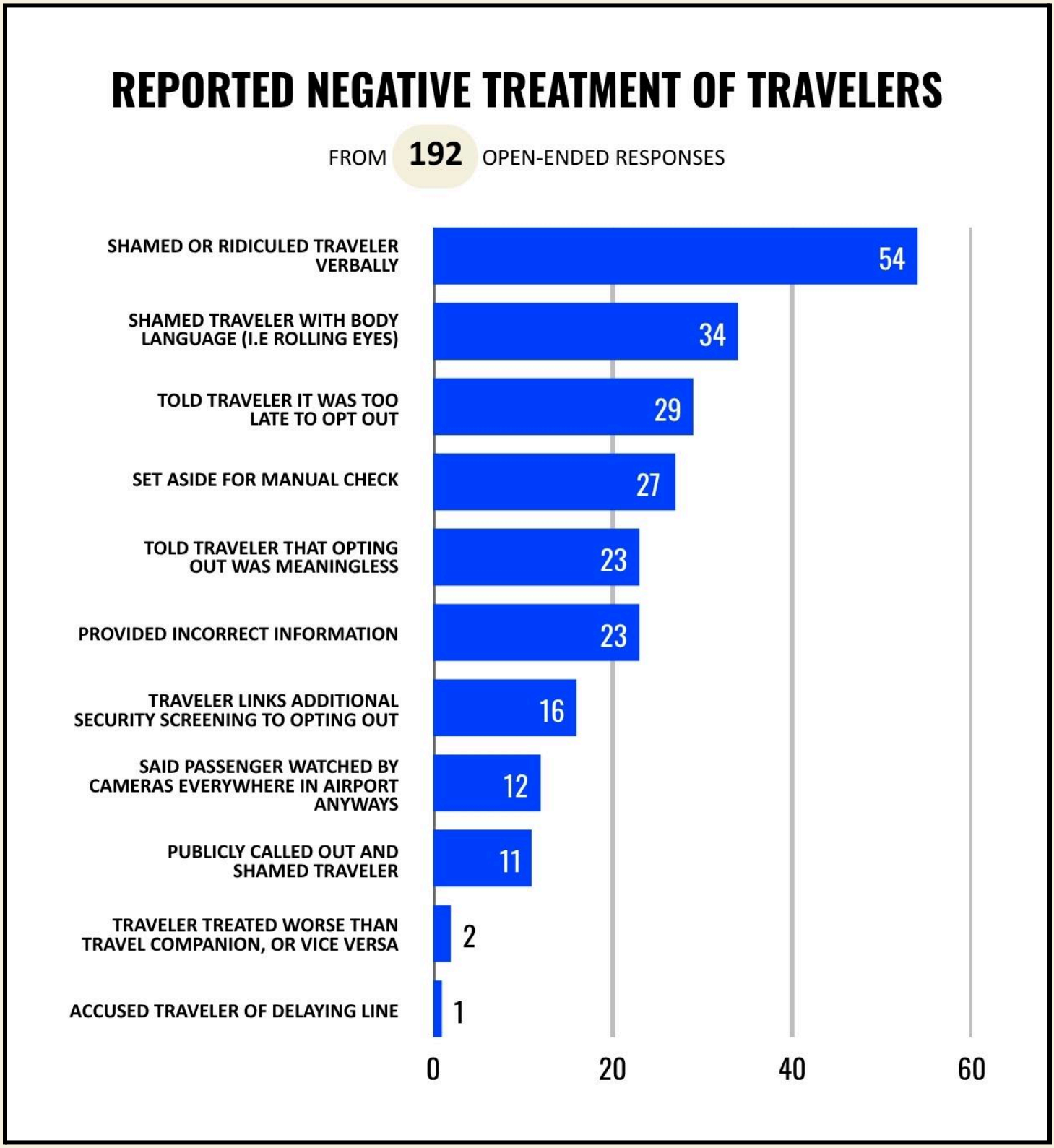
[Figure J] - Treatment by TSA Officers

Positive example of TSA agent treatment:

“The signage I saw explains what to do. If it said you could opt out, I did not see it. I asked, “Can I opt out?” as soon as I handed my id to the agent. He said "That's the way to do it. Some people come up to me and shout ‘no’.” If I hadn’t attended the Freedom Flyers webinar, I would have felt uncomfortable asking.”

- Boston Logan International Airport, September 2024

Negative treatment by TSA agents is broken down in greater depth below:



[Figure K] - Forms of Negative Treatment Reported

The following quotes from travelers help give color to these datapoints:

“I walked up to the TSA agent [...] and didn’t get right in front of the camera. I was instructed to stand in front of it and I told him “no thank you on thank you [sic]” his response was ‘really? That’s ridiculous, you must be stupid’ ”

Seattle-Tacoma International Airport, December 2024

“...I got in line for security and presented my driver’s license to the agent. The agent asked me to stand in front of the camera. Knowing my rights, I asked if I could opt out of the photo. **The agent got angry, raising his voice to tell me that ‘we already took your picture’ and that there are ‘a thousand cameras in this airport . . . there’s a camera in your phone too.’**

I was not interested in arguing with the TSA agent, so I asked if I was good to go and proceeded through security after he waved me through. **The officer did not threaten me with violence or increased wait times, but according to his own admission, he scanned my face in spite of my decision to opt out...”**

Fort Lauderdale-Hollywood International Airport, October 2024

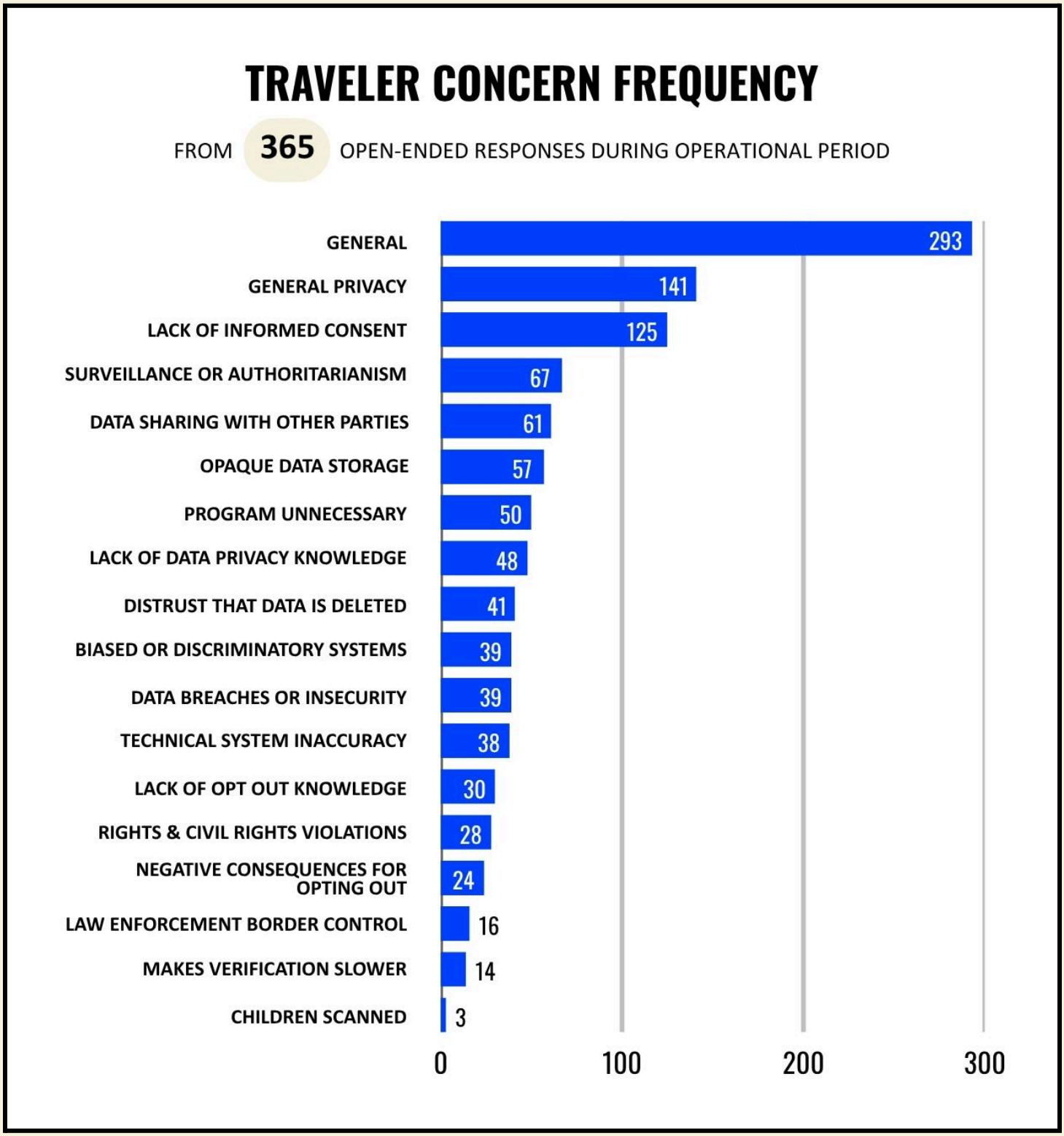
> “TSA agent immediately bereted [*sic*] me. Sighed heavily and made it clear I was inconveniencing him. Visibly angry with me. Sent me to a different agent because he didn't have the right tool. That agent didn't have the right tool either and sent me back to the first agent. I was told I had to wait for them to fetch the right tool, which took approx. 10 min. Was treated with extreme rudeness the entire time.”
>
> **San Francisco International Airport, September 2024**

E. CONCERNS

86.9% of respondents from the operational period (365) shared concerns about the program. Besides the concerns already explored around transparency, consent, and traveler treatment:

- 67 respondents noted concerns about surveillance and authoritarianism.
- 50 respondents shared that they felt the program was not necessary and saw no value in it, with some respondents specifically being concerned that it was a poor use of taxpayer funds.
- 28 respondents expressed concern about civil rights violations.
- 16 respondents shared concerns that data or information from the program could be used by other government enforcement agencies or departments.

All concerns during the operational period are as follows:



[Figure L] - Frequency of Concerns Reported by Travelers

Concern	Count	% of 365	Traveler Commentary
General	293	80.3%	“I don't like people getting my facial data. This is part of the reason I got off Facebook. Not sure if everything was completely removed but in the future privacy would only be for the wealthy. If this is the only wealth I give to my kids, I will do my best.” **Orlando International, September 2024**
General Privacy	141	36.6%	**“**The entire experience left me deeply unsettled. It's concerning how easily people surrender their privacy for the illusion of convenience, unaware they have a choice. It's a stark reminder that we must remain vigilant in protecting our rights, even in the face of seemingly benign procedures.” **El Paso International Airport, September 2024**
Lack of Informed Consent	125	34.3%	“I am concerned that millions of people will be roped into a program that compromises their privacy and uses their likeness without their consent. The signage at the airport was insufficient for passengers who cannot read English or Spanish. If the TSA were concerned about the privacy and security of passengers, they would make it abundantly clear that passengers can opt out. I was in line with half-asleep people who were unlikely to pay close enough attention to a small sign or assert themselves in front of an apathetic TSA agent.” **LaGuardia Airport, June 2024**
Surveillance or Authoritarianism	67	18.4%	**“**... I am also concerned with society's ease and comfort with all the data governments are collecting. Young people have no concern that governments know so much about individuals. As so many people say, it truly feels like Orwell's 1984 novel is no longer dystopian fiction but could become a reality, in some form.” **Denver International Airport, June 2024**

Data Sharing With Other Parties	61	16.7%	"... I am concerned about what agencies/groups might have access to my face data and use it to track me anywhere in the country/world." **Long Beach Airport, September 2024**
Opaque Data Storage	57	15.6%	"I'm positive they're storing that data in some capacity even if they're deleting the raw images. It screams automated racial profiling. I'm constantly concerned with the lack of robust data laws (and the disappearance of checks and balances) within the federal government, and the stakes are only getting higher." **Frederick Douglass Greater Rochester International Airport, October 2024**
Program Unnecessary	50	13.7%	"I have grave concerns about TSA's use of facial recognition. It doesn't increase safety, and like much of TSA, it is safety theater that inconveniences travelers." **Dallas Fort Worth International Airport, June 2024**
Lack Of Data Privacy Knowledge	48	13.2%	I tried to visit the links provided in the signs for information about security and my rights, but ended up in a sea of links and PDFs that made it hard to find any information about the service. **John F. Kennedy International Airport, February 2025**
Distrust that Data is Deleted	41	11.2%	"They say they erase the images but not the datapoints generated from the image and now with large AI models there have been no guarantees that photos will not being [sic] going to train a model before deletion. This is very concerning to me for my right to privacy." **Seattle–Tacoma International Airport, March 2025**
Biased or Discriminatory Systems	39	10.7%	"... I'm concerned about how minority or oppressed groups could be profiled by facial recognition technology." **Cincinnati/Northern Kentucky International Airport, November 2024**

Data Breaches or Insecurity	39	10.7%	"... nor am I obligated to participate in a government sponsored surveillance program in the "promise" that my likeness via photo will not be kept in a data base maintained by the government. I was subject to an OPM data breach back in 2015 when all of my SF-86 information consisting of 10 years of background info for a top secret clearance was hacked and more than likely sold on the dark web. I don't want the government to maintain my biometrics at all." **Yuma International Airport, April 2025**
Technical System Inaccuracy	38	10.4%	"... I am pessimistic that Facial Recognition technology would be an improvement over our current biased world. In fact, I think that poorly trained and misimplemented machines will create more margins of error at an even greater rate than human workers would..." **San Francisco International Airport, August 2024**
Lack of Opt Out Knowledge	30	8.2%	"They really should be making it clear what is happening before you get up there to scan, and I had no idea you could opt out. Everyone should be able to make an informed decision about accepting this or not." **Oakland International Airport, June 2024**
Rights & Civil Rights Violations	28	7.7%	"I consider it a violation of my constitutional rights and I feel it is one more step toward eliminating my constitutional rights completely. The overreach is shocking!" **Kahului Airport, October 2024**
Negative Consequences for Opting Out	24	6.6%	"... Also, not having signage or explanations of what happens if you opt out is very nerve wracking and frankly discouraging in the sense I feel like I have to be opted in." **Denver International Airport, October 2024**
Law Enforcement Border Control	16	4.4%	"Yes, understanding not only the racial biases and inefficacy associated with facial recognition tech but also how my face scan & identity can be both stored

			and shared to LEAs [Law Enforcement Agencies] across the country brings me much concern and pause." **Louis Armstrong New Orleans International Airport, July 2024**
Makes Verification Slower	14	3.8%	"... It does not appear to actually be increasing the ease and speed of security checkpoints, and it results in decreased privacy for everybody." **Boston Logan International Airport, August 2024**
Children Scanned	3	0.8%	"I never want to be scanned or tracked, nor do I want that for my child. No one needs that info and it is clear it will not be used for our benefit, but rather to increase policing and exploitation." **Boston Logan International Airport, June 2024**

F. PROGRAM BENEFITS

8 respondents from the operational period saw benefits from the program, writing that there was no penalty for opting out, verification was faster, security was enhanced, there was sufficient information about the program, or the technology was accurate.

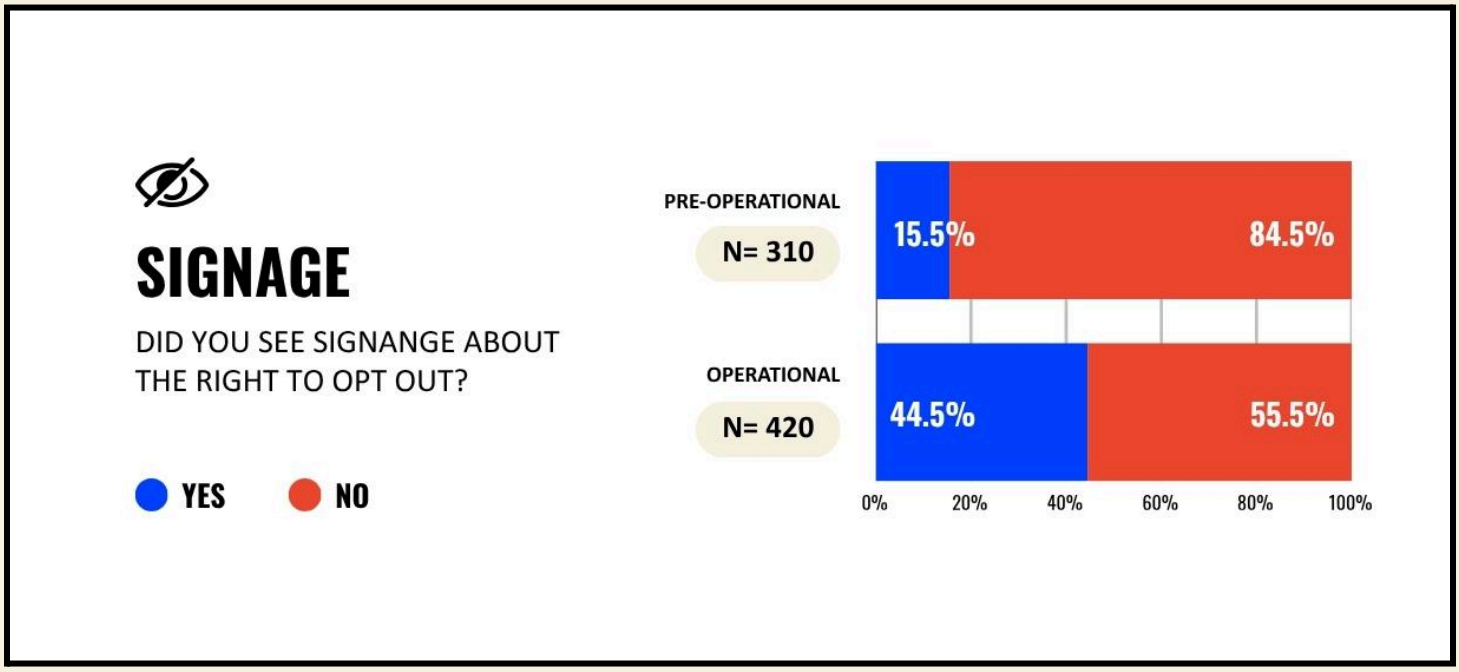
5 travelers wrote that they either did not have concerns or did not yet have concerns in open-ended responses.

G. PRE- AND POST-OPERATIONAL CHANGES

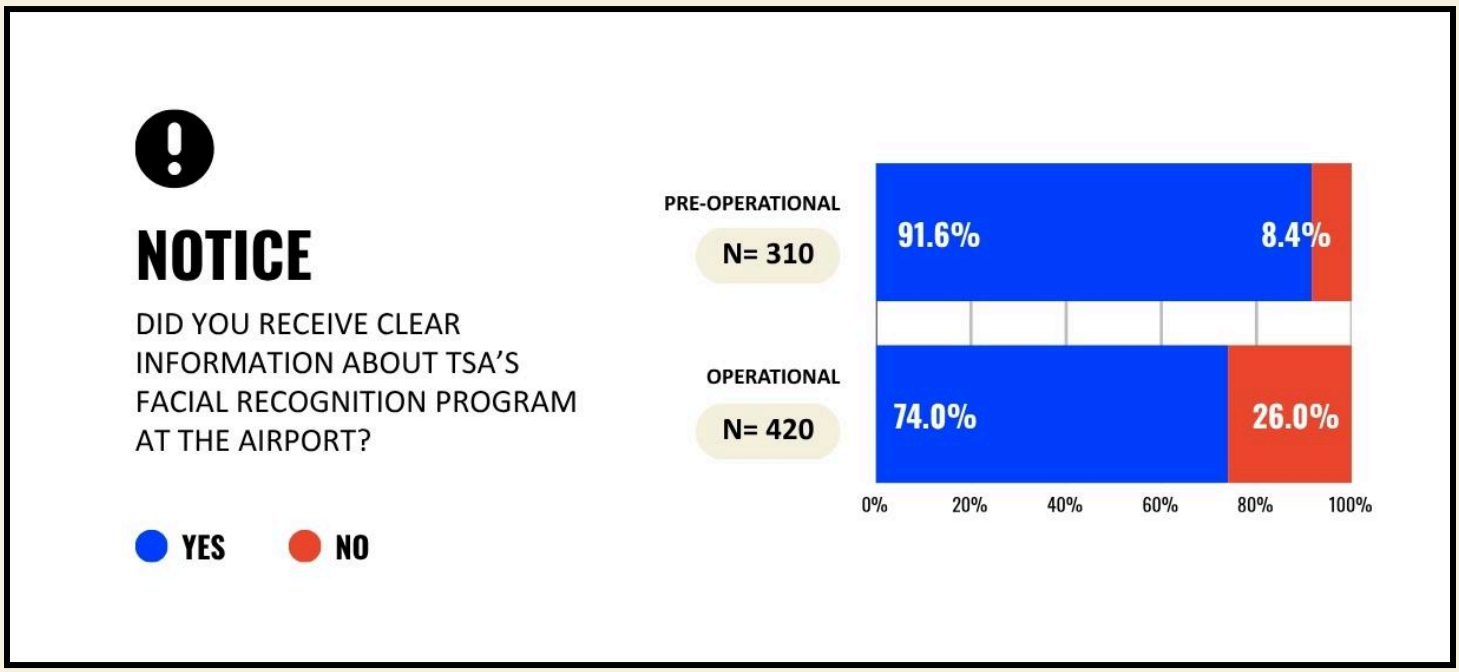
From 2023 through February 2024, AJL surveyed travelers on their experience before TSA's facial recognition program was considered fully operational. In this section, we compare responses to close-ended questions before and after the program was operational.

We identified 310 responses from the pre-operational data to compare against the 420 responses we gathered in the operational time period.

Traveler reports of signage and notice improved from the pre-operational period to operational period.

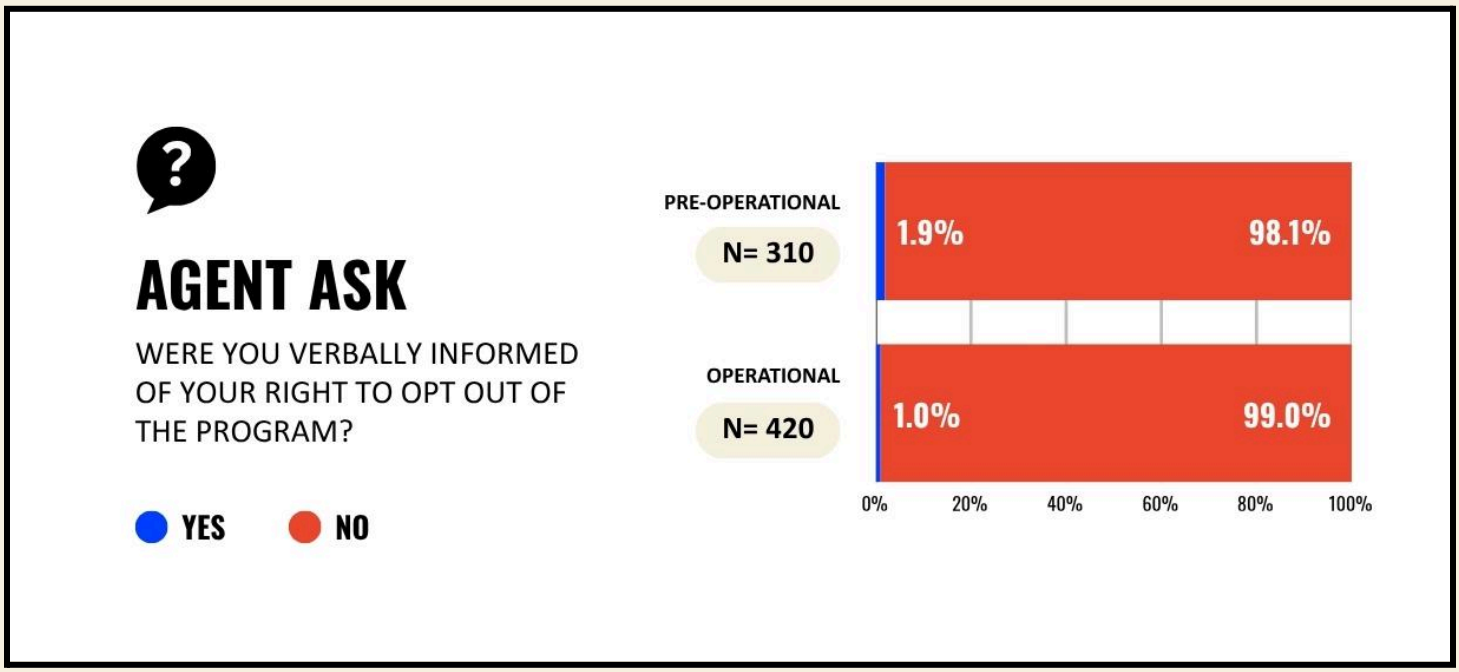


[Figure M] - Proportions of Respondents Who Saw Signage About Opting Out of Facial Recognition Before and After Operational Period Began



[Figure N] - Proportions of Respondents Who Received Information about Facial Recognition Before and After Operational Period Began

However, traveler reports of whether they were verbally informed of their right to opt out of the program remained very low and slightly decreased.



[Figure O] - Proportion of Respondents Verbally Informed of Their Right to Opt Out Before and After Operational Period Began

BOSTON LOGAN INTERNATIONAL AIRPORT

During the operational period, we received 49 submissions from travelers at Boston Logan International Airport (BOS) regarding their experiences with TSA's use of facial recognition. Boston is also home to the Algorithmic Justice League and digital rights organizations like Fight for the Future [47]. We summarize survey results for Boston Logan below:

Signage:

- 14 travelers reported seeing signage containing opt-out information.
- 35 travelers did not see signage.
- When describing their experience, 10 travelers noted that signage was missing, difficult to find, or incomplete.

Notice:

- 8 travelers reported receiving notice about the program.
- 41 travelers reported that they did not receive notice.
- 0 travelers were verbally informed of their right to opt out of the program.

Opting Out:

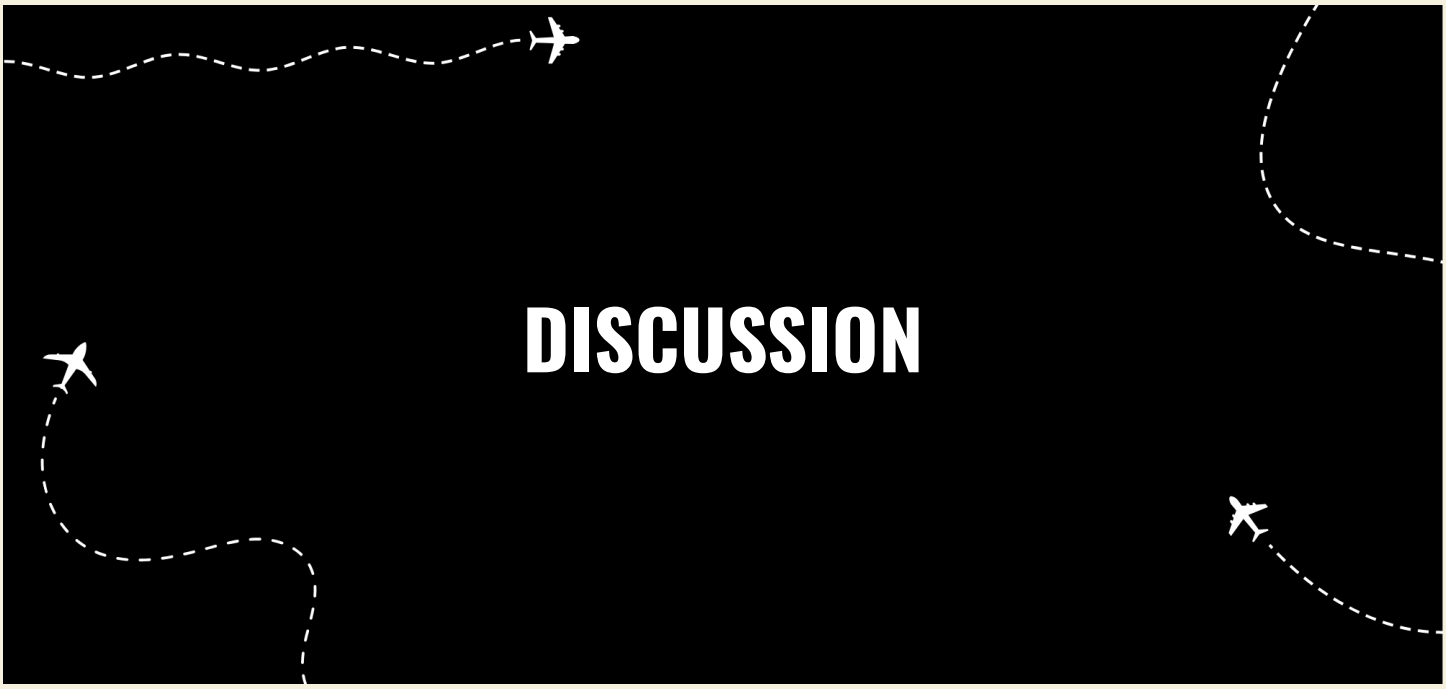
- 30 travelers requested to opt out.
    - 21 travelers indicated that they successfully opted out.
- 14 travelers were scanned before they had a chance to opt out.
- 8 travelers did not know opting out was an option.
- 4 travelers did not feel comfortable opting out, and may have felt fear of possible consequences.
- 1 passenger did not request to opt out.

Treatment:

- 12 travelers indicated that TSA officers treated them with respect.
- 5 travelers reported being shamed by TSA officers after requesting to opt out, including one who was accused of delaying other travelers.
- 3 travelers believed they were subjected to secondary security screening as a result of opting out.
- 2 travelers were told by officers that it was too late to opt out.

Concerns:

- 39 travelers indicated concerns about the program.
- 16 respondents indicated fundamental concerns over the program which have no technical fixes: privacy, civil rights, and surveillance or authoritarianism.
- 12 travelers indicated concerns over data handling and data privacy practices.
- 9 travelers indicated concerns over a lack of informed consent.
- 7 travelers indicated concerns over biased or discriminatory systems.
- 6 travelers indicated that they did not believe the program was necessary.



The findings on program transparency, consent processes, and TSA officer treatment of travelers across domestic airports reveal glaring gaps between the vision of friction-free travel shared by TSA and the lived experiences of hundreds of travelers. In the 2018 TSA Biometrics Roadmap report, the agency outlined a future where travelers seamlessly walk through the airport and are scanned by cameras to confirm identities with the promise of increased efficiency [48]. In the outline of phases for the program, the final vision is to make biometric identification using facial recognition the default way to verify travelers in the United States.

The integration of facial recognition technology into airport travel thus far is done with inconsistent transparency, a lack of robust public deliberation, and a litany of documented violations of principles of consent and expectations of dignity.

When evaluated against TSA's own ideals and stated policies, the story that agency officials tell about the program and the scorecards that the Algorithmic Justice League has collected reveal instructive contradictions.

TSA POLICY SUMMARY

"TSA policy requires that [Transportation Security Officers] TSOs show each traveler respect and ensure their privacy is protected. Travelers who do not wish to participate in the facial recognition technology process may decline the optional photo, without recourse, in favor of an alternative identity verification process, which does not use facial recognition technology to verify their identity.

This action will not take longer and travelers will not lose their place in line for security screening. TSA is committed to protecting traveler privacy, civil rights, civil liberties and ensuring the public's trust as it seeks to improve the traveler experience through its exploration of identity verification technologies."

TSA Factsheet on Facial Recognition Technology, accessed June 30, 2025 [49]

KEY CONCLUSION:

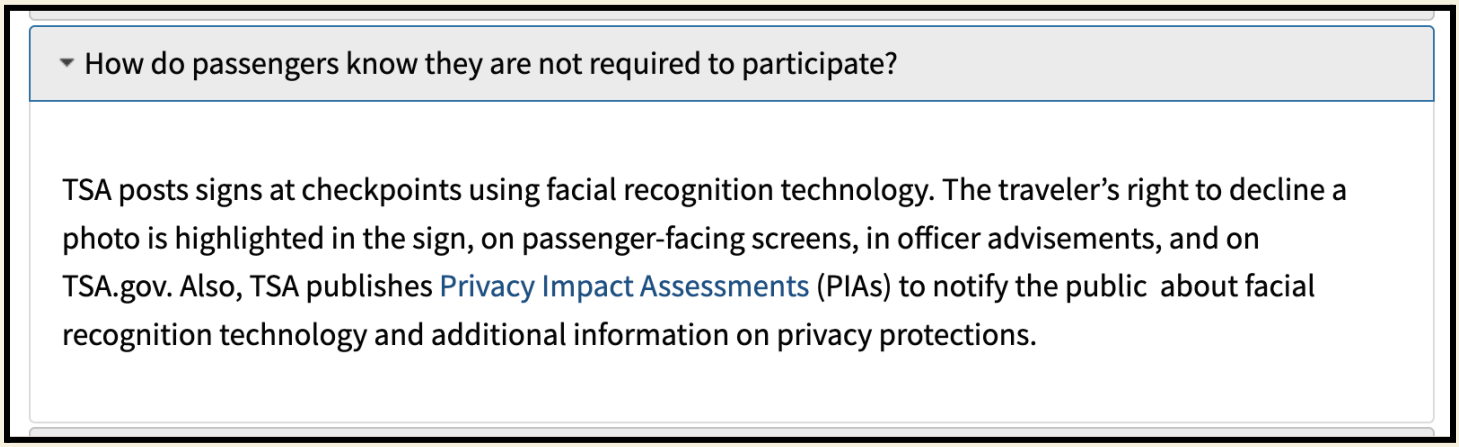
Many travelers across 91 US airports experience the TSA Facial Recognition Program as mandatory though it is presented by the agency officials as voluntary.

Though the program is presented as voluntary and the May 2025 PCLOB Report on TSA Use of Facial Recognition recommends the program remain voluntary, many travelers assume submitting to airport face scans is mandatory.

The assumption of mandatory participation is reinforced at times by both the behavior of TSA officers and the implementation of the materials and technology that facilitate the program execution. Some TSA officers erroneously inform travelers the program is mandatory.

> “I requested to opt out, and they informed me that “since January 1st, it is mandatory”. I said “I do not consent,” they repeated the previous sentence. I had my face scanned.“

Signage is the main mechanism used to inform travelers about the program and their right to opt out before they reach the cameras.



[Figure P] - Screenshot of TSA FAQs on Biometric Technology, accessed June 30, 2025 [50]

TSA is aware of the risk that photos may be taken without the awareness of the traveling public when facial recognition is deployed in a biometric proof-of-concept program. The 2020 TSA Privacy Impact Assessment (PIA) on Travel Documented Checker Using Automated Facial Verification [51] states:

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

2020 Privacy Impact Assessment DHS/TSA/PIA-046(b) TDC Automation Using Facial Verification [51]

This PIA proposed signage as a mitigation to the acknowledged privacy risk:

"This risk is mitigated. The process for taking the photograph is completely overt and obvious since it requires the passenger's cooperation to pose for the photo in front of the camera.

In addition, **this PIA, along with signs posted in close proximity to the CAT-C and public communications materials, will inform members of the public of the procedures for participating** and that TSA will take their photo and attempt to match the facial image with the biometric image from their identity document. Signage and public communications materials will also inform members of the public of their ability to seek manual procedures if they do not wish to participate in the proof of concept"

2020 Privacy Impact Assessment DHS/TSA/PIA-046(b) TDC Automation Using Facial Verification [51]

Based on the evidence gathered in this report, the 2020 mitigation strategy is insufficient.

KEY CONCLUSION:

Informed Consent is not consistently achieved by the TSA Facial Recognition Program. Many travelers are not informed about the opt out implementation of the program and/or given the opportunity to opt out.

Indeed, these concerns are echoed by travelers' lived experience. Signage is at times missing, or when present, difficult to read, incomplete or present impractical links to learn more about the technology moments before being told to "step up to the camera" by an authority figure.

For example, to learn about the privacy and security protections that have been put in place for TSA PreCheck® Touchless ID, a user is directed to see TSA's Privacy Impact Assessments (PIAs). (https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa [52]). On that web page, 48 PIAs are listed. If a user knows that TSA uses the term "Credential Authentication Technology (CAT)" to at times indicate the use of facial recognition, they may then locate the *DHS/TSA/PIA-024 Credential Authentication Technology/Boarding Pass Scanning System (CAT/BPSS)* which at the time of writing was listed 20th out of 48 links. Following the link to compliance documents: https://www.dhs.gov/publication/catbpss-update [53], the user is then faced with two documents that indicate a focus on CAT. The first is from 2013 [54] and the second is from 2009 [55]. According to PCLOB, TSA began exploring the use of facial recognition in aviation in 2017 [1].

Should the user persist, they may scroll down to the 40th item in the unnumbered list and locate the DHS/TSA/PIA-046 Travel Document Checker Automation Using Facial Identification https://www.dhs.gov/publication/dhstsapia-046-travel-document-checker-automation-using-facial-recognition [56]. On this page, there are 5 documents that indicate either the use of facial identification, facial verification, or facial recognition with the earliest document posted in 2018 and the latest document posted in 2022 with a note that a small update was added in 2023.

Even when travelers see clear signage, there is still discomfort in needing to explicitly opt out when faced with authoritative direction to submit their biometric information through a face scan and the feeling of social pressure of long lines.

> "There was only one sign when entering the TSA line that was easy to miss and the sign above the agent's desk. I didn't feel that there was any meaningful information about the FRT[facial recognition] usage, and the agent automatically was scanning everyone's faces before me without even asking them.

The social norm in place was to just quietly accept the FRT scan so deviating from that norm felt uncomfortable. The signage was also vague and unclear - anyone in a rush to get through to their flight would miss it, and I'm certain many did…"

Given that 99% of respondents shared that they did not receive verbal information about the right to opt out, 56% did not see signage about the right to opt out, and 20% had their faces scanned before they could even opt out, the voluntary nature of the program is compromised. Bipartisan lawmakers' concern that "TSA continues to shuttle people through its new facial recognition system," without notice of its voluntary nature, is further supported by these scorecard findings.[7]

KEY CONCLUSION:

Some travelers face verbal abuse, hostile body language, increased scrutiny, and other injuries to dignity and respect when attempting to opt out.

According to the TSA, the agency's personnel are trained to treat every passenger with dignity and respect [49], [59]. The scorecards indicate repeated instances across different airports of passengers being shamed verbally or with body language and passengers facing ridicule. Some travelers also believe that because they choose to opt out, they face additional undue scrutiny and security screening. The TSA website states that when someone opts out, they should not face additional wait times or lose their place in line. Additionally, some TSA officers actively undermined the successful opt out of travelers, by implying through body language or verbally that there are other cameras observing the travelers.

[7] Senator Jeff Merkley's video report on a trip at Reagan National Airport, where he shows missing signage and emphasizes how difficult it would be for passengers to find information on opting out [57]. See also his video trip report from 2025 [58] and Congressional letters from him and other bipartisan lawmakers on the issue [13], [35].

> I asked the agent to opt out. She pointed to a security camera in the ceiling and said, “you can’t opt out of that one.” I replied, “yes but that one doesn’t collect my face print.”

The fear of poor treatment paired with continuous affront to dignity and active shaming raise a serious flag on the training protocols and adherence to internal professional standards.

RECOMMENDATIONS

We conclude with recommendations on the TSA's experimental deployment of facial recognition on the traveling public.

HALT FACIAL RECOGNITION EXPERIMENT

Most importantly, the Algorithmic Justice League recommends a halt of the TSA's use of facial recognition to allow for public deliberation and to address the concerns raised by the traveling public, civil society organizations, bipartisan elected officials, and even the U.S. government's own Privacy and Civil Liberties Oversight Board (PCLOB).

According to PCLOB, "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" [1, p. 6]. Despite more recent efforts to inform the public about the expansion of FRT and the options to opt out, "there has been a lack of clear communication about the nature and maturity of plans for deployment of FRT" [1, p. 4].

The PCLOB report highlights the potential for surveillance expansion and normalization, by stating, “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. 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” [1, p. 44].

The PCLOB report includes a recommendation that “TSA and DHS should establish procedures for collecting, investigating, and responding to FRT-related inquiries and complaints from travelers” [1, p. 110]. In addition to outlining the procedures to track and respond to individual traveler queries and complaints, the PCLOB report recommends that “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” [1, p. 110].

While the TSA should set up more robust channels to field the concerns of travelers, AJL’s Comply To Reply? Report findings provide a body of evidence to inform immediate and near-term action.

AJL’s recommendations to policy makers and TSA leadership build upon the PCLOB report and draw on the lived experiences of hundreds of U.S. airport travelers from March 2024 until June 2, 2025. AJL recommendations are organized around three broad pillars: (1) Increase freedom and oversight, and preserve privacy, (2) Promote informed public decision making, and (3) Prevent and redress disrespectful treatment.

#1 PRESERVE FREEDOM AND PRIVACY

Recognizing that the expansion of the use of facial recognition technologies (FRTs) on members of the public requires careful public consideration and government oversight and regulation, AJL calls for an immediate halt of the use of FRT at TSA Checkpoints to allow for public deliberation and addressing the issues raised by the PCLOB report and by external experts. High risk technologies with the potential for mass biometric surveillance should never be mandatory, and the evidence of benefits should outweigh documented harm and credible risks. Experimental technologies or pilots must require Congressional approval for the trial phase, and further approval for adoption and expansion. Given that the 1:N program has greater potential for expansion and impact on privacy and civil liberties, extensive public awareness and deliberation are a must prior to any consideration of deployment. Protection of the public's privacy is key, with a need for strong data protection policies.

AJL's recommendations in this category are:

Oversight

- Halt the use of facial recognition technology at domestic checkpoints by TSA.
- Conduct a comprehensive and independent Privacy Impact Assessment for the use of FRTs on the traveling public at airports.
- Conduct retrospective independent audits of the efficacy of the program with results shared with policy makers and the general public.
- Release retrospective comprehensive statistics on the technical performance metrics of the program including false positives and false negatives by age, race, gender, and other demographics previously captured.

Privacy and Freedom

- Given that TSA's use of FRT involves multiple systems that handle traveler information (TSA's Secure Flight, the TSA CAT-2 device, DHS S&T, and CBP's TVS in the case of 1:N identification) [1, p. 4], ensure a robust data protection policy so that the public's data cannot be accessed by third parties or hackers, or used for purposes beyond immediate travel.
- Require transparency and public notification about data sharing, retention, and storage policies, including the role of private vendors and the error rates of proprietary algorithms.

#2 PROMOTE INFORMED PUBLIC DECISION MAKING

Any experimental biometrics program, if congressionally approved, must be set up as opt-in. Opt-out does not work, given the perception among travelers that the program is mandatory and given the power imbalances between the traveler and the TSA officer. In order to be perceived as trustworthy, any program must be developed with full public knowledge and informed decision making, and without perceived coercion.

AJL's recommendations in this category are:

Opt-In and Voluntary

- Following public deliberation and congressional approval, any biometric programs judged to be beneficial should remain strictly voluntary, require an explicit opt-in, and provide clear alternatives.
    - The standard manual verification process should always be available and explicitly offered.

Public Awareness

- Develop, implement, and evaluate a mechanism for informed consent. Ensure that all travelers have the opportunity to know about the program (taking into account disabilities, languages spoken, and other traveler needs)--examples could include use of intercom in addition to signage, use of multiple languages to reach diverse audiences.

- Require that minors always be screened visually by the TSA officer and not by a facial recognition device.

- Address knowledge gaps and clarify terminology for travelers on the TSA website and with clear signage in the airport prior to arrival at the TSA airport checkpoint.

- Ensure public transparency on the use of technology, including data retention and protection practices, performance accuracy error rates, and a clear communication of the risks and benefits.

#3 PREVENT & REDRESS DISRESPECTFUL TREATMENT

Given the feedback received from hundreds of travelers across 91 airports in the U.S., AJL calls for immediate and actionable steps to be undertaken by TSA to ensure respect and dignity for all travelers. Millions of people across the U.S. travel daily for professional and personal purposes, with little understanding of how the FRT program operates and little recourse when experiencing disrespectful treatment at the hands of TSA officers if they wish to exercise their right to opt out.

AJL's recommendations in this category are:

Training and Assessment

- By December 2025, develop dedicated biometrics complaint procedure opportunities for travelers to submit new and retroactive complaints specifically related to the TSA use of FRTs and any other experimental biometric pilot and develop specific procedures to respond to submissions.
    - Track demographics and ensure travelers' experiences with TSA officers and technologies are grounded in respect for human dignity and rights.
- By December 2025, develop, implement, and evaluate traveler dignity protocols, and provide training for and evaluation of TSA officers to ensure adherence to such standards.

Bipartisan lawmakers question the necessity of the facial recognition program [35], privacy advocates campaign against the rise of societal adoption of biometric surveillance technologies that reach in and beyond airports [17], [18], and now hundreds of travelers document the reality of encountering airport face scans. AJL's goal is to center choice, agency, and rights of the traveling public and it is our hope that the research and recommendations in this report will help us communicate to and build greater awareness among policy makers, civil society, and members of the traveling public about biometric rights in aviation and public life.

REFERENCES

[1] Privacy and Civil Liberties Oversight Board, “Use of Facial Recognition Technology by the Transportation Security Administration: Staff Report,” Privacy and Civil Liberties Oversight Board, May 2025. Available: https://www.pclob.gov/reports/tsa-facial-recognition-2025

[2] “You Can Opt Out of TSA Face Scans,” *The Algorithmic Justice League*. Available: https://www.ajl.org/campaigns/fly. [Accessed: Jun. 30, 2025]

[3] “TSA Scorecard,” *Algorithmic Justice League*. Available: https://report.ajl.org/tsa-scorecard. [Accessed: Jun. 30, 2025]

[4] Dr. Joy Buolamwini, “Civil Rights Implications of the Federal Use of Facial Recognition Technology,” U.S. Commission on Civil Rights, Mar. 2024. Available: https://www.ajl.org/civil-rights-commission-written-testimony

[5] *Freedom Flyers Summit: Resisting Airport Face Scans*, (Jul. 19, 2024). Available: https://www.youtube.com/watch?v=3rU5CxYhLzs. [Accessed: Jun. 30, 2025]

[6] Algorithmic Justice League, “2024 TSA Scorecard Preliminary Results,” presented at the RightsCon 2025, Taipei, Taiwan.

[7] *Aviation and Transportation Security Act of 2001*. 2001, p. 597.

[8] “Transportation Security Administration Transition to Department of Homeland Security; Technical Amendments,” *Fed. Regist.*, vol. 68, no. 160, pp. 49718–49723, Aug. 2003, Available: https://www.federalregister.gov/documents/2003/08/19/03-20927/transportation-security-administration-transition-to-department-of-homeland-security-technical

[9] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*. 2001, p. 272. Available: https://www.congress.gov/bill/107th-congress/house-bill/3162

[10] European Union, *Artificial Intelligence Act*, vol. 2024/1689. 2024. Available: https://artificialintelligenceact.eu/article/5/

[11] Joy Buolamwini, Vicente Ordóñez, Jamie Morgenstern, and Erik Learned-Miller, “Facial

Recognition Technologies: A Primer," Algorithmic Justice League, May 2020. Available: https://www.ajl.org/federal-office-call
[12] Jeffrey A. Merkley, Edward J. Markey, Cory A. Booker, Elizabeth Warren, and Bernard Sanders, "Letter to Administrator David Pekoske Regarding TSA Facial Recognition Technology," Feb. 09, 2023. Available: https://www.merkley.senate.gov/wp-content/uploads/imo/media/doc/tsa_facial_recognition_technology_letter.pdf
[13] Jeffery A. Merkley *et al.*, "Letter to Senate Leadership Urging Restrictions on TSA Facial Recognition Technology in FAA Authorization," May 02, 2024. Available: https://www.merkley.senate.gov/wp-content/uploads/2024_05_02_LTR-TSA-Freeze-to-Leadership.pdf
[14] *Committee Amendment to H.P. 1174, L.D. 1585, "An Act To Increase Privacy and Security by Regulating the Use of Facial Surveillance Systems by Departments, Public Employees and Public Officials."* 2021. Available: https://www.mainelegislature.org/legis/bills/getPDF.asp?paper=HP1174&item=2&snum=130
[15] "Boston becomes largest city on East Coast to ban face surveillance," *ACLU Massachusetts*, Jun. 24, 2020. Available: https://www.aclum.org/en/press-releases/boston-becomes-largest-city-east-coast-ban-face-surveillance. [Accessed: Jun. 30, 2025]
[16] Kate Conger, Richard Fausset, and Serge F. Kovaleski, "San Francisco Bans Facial Recognition Technology," *The New York Times*, May 14, 2019. Available: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html. [Accessed: Jun. 30, 2025]
[17] "Ban Facial Recognition," *Fight for the Future*. Available: https://banfacialrecognition.com. [Accessed: Jun. 30, 2025]
[18] Jason Kelley, "Fighting Back Against Face Surveillance in the Skies: 2019 Year in Review," *Electronic Frontier Foundation*, Dec. 27, 2019. Available: https://www.eff.org/deeplinks/2019/12/fighting-back-against-face-surveillance-skies-year-review-2019
[19] "Know Your Rights | Enforcement at the Airport," *American Civil Liberties Union*. Available: https://www.aclu.org/know-your-rights/what-do-when-encountering-law-enforcement-airports-and-other-ports-entry-us. [Accessed: Jun. 30, 2025]
[20] "Face Surveillance," *Electronic Privacy Information Center*. Available: https://archive.epic.org/privacy/surveillance/face-surveillance/. [Accessed: Jun. 30, 2025]
[21] Shira Ovide, "You can say no to a TSA face scan. But even a senator had trouble.," *The Washington Post*, Jul. 11, 2023. Available: https://www.washingtonpost.com/technology/2023/07/11/tsa-airport-security-facial-recognition/. [Accessed: Jun. 30, 2025]
[22] Mark Sullivan, "This TikTok creator is showing that opting out of TSA face scans isn't always easy," *Fast Company*, Aug. 16, 2024. Available: https://www.fastcompany.com/91173990/tiktok-creator-opting-out-of-tsa-face-scans. [Accessed: Jun. 30, 2025]
[23] "Cybersecurity Resource Center," *U.S. Office of Personnel Management*. Available: https://www.opm.gov/cybersecurity-resource-center/. [Accessed: Jun. 30, 2025]
[24] Office of Inspector General, "Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot," Department of Homeland Security, OIG-20-71, Sep. 2020. Available:

https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf
[25] *Katz v. United States*, vol. 389 U.S. 347. 1967.
[26] "Know Your Rights | Enforcement at the Airport," *American Civil Liberties Union*. Available: https://www.aclu.org/know-your-rights/what-do-when-encountering-law-enforcement-airports-and-other-ports-entry-us. [Accessed: Jun. 30, 2025]
[27] Tendayi Achiume, UN. Human Rights Council. Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, and UN. Secretary-General, Eds., *Contemporary forms of racism, racial discrimination, xenophobia and related intolerance: note*. New York: UN, 28. Available: https://digitallibrary.un.org/record/3893019. [Accessed: Jun. 30, 2025]
[28] Sasha Costanza-Chock, "Design Justice, A.I., and Escape from the Matrix of Domination," *J. Des. Sci.*, Jul. 2018, doi: 10.21428/96c8d426. Available: https://jods.mitpress.mit.edu/pub/costanza-chock. [Accessed: Jun. 30, 2025]
[29] Sandy E. James, Jody L. Herman, Laura E. Durso, and Rodrigo Heng-Lehtinen, "Early Insights: A Report of the 2022 U.S. Transgender Survey," National Center for Transgender Equality, Washington, DC, Feb. 2024. Available: https://transequality.org/sites/default/files/2024-02/2022%20USTS%20Early%20Insights%20Report_FINAL.pdf
[30] Alyxaundria Sanford, "Artificial Intelligence is Putting Innocent People at Risk of Being Incarcerated," *Innocence Project*. Available: https://innocenceproject.org/news/artificial-intelligence-is-putting-innocent-people-at-risk-of-being-incarcerated/. [Accessed: Jun. 30, 2025]
[31] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," in *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, PMLR, Jan. 2018, pp. 77–91. Available: https://proceedings.mlr.press/v81/buolamwini18a.html. [Accessed: Jun. 30, 2025]
[32] Joy Buolamwini, *Unmasking AI: my mission to protect what is human in a world of machines*. New York: Random House, 2023.
[33] "CBC Expresses Privacy, Racial Bias Concerns about Facial Recognition Technology Marketed, Sold by Amazon," *Congressional Black Caucus*, May 24, 2018. Available: https://cbc.house.gov/news/documentsingle.aspx?DocumentID=898. [Accessed: Jun. 30, 2025]
[34] Joy Buolamwini, "The Face Is the Final Frontier of Privacy," *TIME*, Nov. 21, 2023. Available: https://time.com/6338338/joy-buolamwini-ai-face-privacy/. [Accessed: Jun. 30, 2025]
[35] Jeffrey A. Merkley *et al.*, "Letter to DHS Inspector General Regarding TSA Facial Recognition Technology," Nov. 20, 2024. Available: https://www.merkley.senate.gov/wp-content/uploads/Merkley-Letter-to-IG-FINAL.pdf
[36] *Mission: Impossible - Dead Reckoning Part One*, (2023). Available: https://www.imdb.com/title/tt9603212. [Accessed: Jun. 30, 2025]
[37] "See No Evil," Arrow Media and Saloon Media, 2014. Available: https://www.imdb.com/title/tt4189570/. [Accessed: Jun. 30, 2025]
[38] "The future is here: iPhone X - Apple," *Apple*. Available: https://www.apple.com/newsroom/2017/09/the-future-is-here-iphone-x/. [Accessed: Jun. 30, 2025]
[39] "American Airlines now offers TSA PreCheck Touchless ID for AAdvantage members at select airports." Available:

https://news.aa.com/news/news-details/2025/American-Airlines-now-offers-TSA-PreCheck-Touchless-ID-for-AAdvantage-members-at-select-airports-AADV-05/default.aspx. [Accessed: Jul. 02, 2025]

[40] Cynthia M. Cook, Laurie Cuffney, John J. Howard, Yevgeniy B. Sirotin, Jerry L. Tipton, and Arun R. Vemury, "Performance Differentials in Deployed Biometric Systems Caused by Open-Source Face Detectors," in *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*, Athens Greece: ACM, Jun. 2025, pp. 2630–2639. Available: https://dl.acm.org/doi/10.1145/3715275.3732171. [Accessed: Jul. 01, 2025]

[41] Cynthia M. Cook, John J. Howard, Yevgeniy B. Sirotin, Jerry L. Tipton, and Arun R. Vemury, "Demographic Effects Across 158 Facial Recognition Systems," U.S. Department of Homeland Security, Science and Technology Directorate, DHS S&T Technical Paper Series, Aug. 2023. Available: https://www.dhs.gov/sites/default/files/2023-09/23_0926_st_demographic_effects_across_158_facial_recognition_systems.pdf

[42] Patrick Grother, "Face Recognition Vendor Test (FRVT) Part 8: Summarizing Demographic Differentials," National Institute of Standards and Technology, NIST IR 8429 ipd, Jul. 2022. Available: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8429.ipd.pdf. [Accessed: Jul. 01, 2025]

[43] Patrick Grother, Mei Ngan, and Kayee Hanaoka, "Face Recognition Vendor Test Part 3: Demographic Effects," National Institute of Standards and Technology, NIST IR 8280, Dec. 2019. doi: 10.6028/NIST.IR.8280. Available: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf. [Accessed: Jul. 01, 2025]

[44] Dominique Farrell, "Facial recognition software in airports raises privacy and racial bias concerns," *GBH*, Jun. 16, 2023. Available: https://www.wgbh.org/news/national/2023-06-16/facial-recognition-software-in-airports-raises-privacy-and-racial-bias-concerns. [Accessed: Jul. 01, 2025]

[45] Sydney Bauer, "Trans travelers face 'invasive' airport security at Thanksgiving," *Reuters*, Nov. 28, 2019. Available: https://www.reuters.com/article/world/trans-travelers-face-invasive-airport-security-at-thanksgiving-idUSKBN1Y222Y/. [Accessed: Jul. 01, 2025]

[46] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*. Washington, D.C.: National Academies Press, 2024. Available: https://www.nap.edu/catalog/27397. [Accessed: Jul. 01, 2025]

[47] "Fight for the Future," *Fight for the Future*. Available: https://www.fightforthefuture.org/. [Accessed: Jul. 01, 2025]

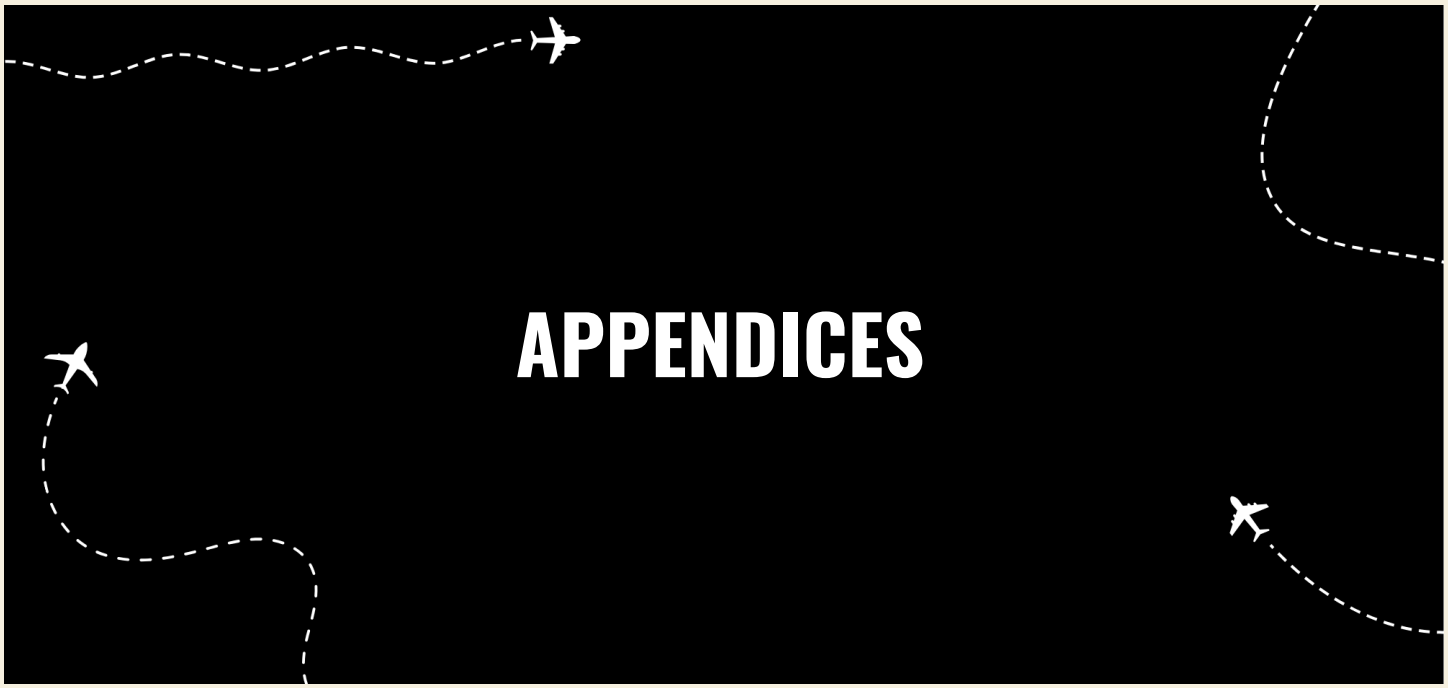
[48] "TSA Biometrics Roadmap for Aviation Security & the Passenger Experience," Transportation Security Administration, Sep. 2018. Available: https://www.govinfo.gov/content/pkg/GOVPUB-HS4_300-PURL-gpo110235/pdf/GOVPUB-HS4_300-PURL-gpo110235.pdf

[49] "Facial Recognition Technology," *Transportation Security Administration*. Available: https://www.tsa.gov/news/press/factsheets/facial-recognition-technology. [Accessed: Jun. 30, 2025]

[50] "Biometrics Technology," *Transportation Security Administration*. Available: https://www.tsa.gov/biometrics-technology. [Accessed: Jun. 30, 2025]

[51] "Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Verification," U.S. Department of Homeland Security, Transportation Security Administration,

Privacy Impact Assessment DHS/TSA/PIA-046(b), Jun. 2020. Available: https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa046b-tdc-june2020.pdf
[52] "Privacy Documents for TSA," *Homeland Security*. Available: https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa. [Accessed: Jul. 01, 2025]
[53] "CAT/BPSS Update," *Homeland Security*. Available: https://www.dhs.gov/publication/catbpss-update. [Accessed: Jul. 01, 2025]
[54] "Privacy Impact Assessment Update for Credential Authentication Technology/ Boarding Pass Scanning System," Department of Homeland Security, DHS/TSA/PIA-024(b). Available: https://www.dhs.gov/sites/default/files/publications/privacy_pia%20update_tsa_cat%20bpss_20130118_0.pdf
[55] "Privacy Impact Assessment Update for Credential Authentication Technology/Boarding Pass Scanning System," Department of Homeland Security, DHS/TSA/PIA-024(a), Aug. 2009. Available: https://www.dhs.gov/sites/default/files/publications/privacy_pia_tsa_catbpss.pdf
[56] "DHS/TSA/PIA-046 Travel Document Checker Automation Using Facial Identification," *Department of Homeland Security*. Available: https://www.dhs.gov/publication/dhstsapia-046-travel-document-checker-automation-using-facial-recognition. [Accessed: Jul. 01, 2025]
[57] "Senator Jeff Merkley on Instagram: 'I was flying out of DCA...,'" *Instagram*, Sep. 01, 2023. Available: https://www.instagram.com/senjeffmerkley/reel/CvYKJjsgRqn/. [Accessed: Jul. 02, 2025]
[58] "Senator Jeff Merkley on Instagram: 'Reminder: you CAN opt-out...,'" *Instagram*, Feb. 14, 2025. Available: https://www.instagram.com/senjeffmerkley/reel/DGCJPIZPm9v/. [Accessed: Jul. 02, 2025]
[59] "Is TSA using facial identification recognition technology to profile and deport passengers?," *Transportation Security Administration*. Available: https://www.tsa.gov/travel/frequently-asked-questions/tsa-using-facial-identification-recognition-technology-profile. [Accessed: Jul. 01, 2025]
[60] Andrea Dean, "Deploying Software: A Technology Explainer and a Look Toward the Future," *Georget. Law Technol. Rev.*, vol. 9, p. 667, 2025, Available: https://georgetownlawtechreview.org/wp-content/uploads/2025/05/Andrea.Dean_DEPLOYING-SOFTWARE_2025.pdf. [Accessed: Jul. 02, 2025]
[61] Privacy and Civil Liberties Oversight Board, "Press Release on Termination of PCLOB Chair and Members," Privacy and Civil Liberties Oversight Board, Press Release, Jan. 2025. Available: https://documents.pclob.gov/prod/Documents/EventsAndPress/994df0d6-6bae-4284-a95f-3f3699e0a0f0/PCLOB%20press%20release%20(1-27-25)%20-%20508%20Complete.pdf
[62] *LeBlanc v. US PCLOB*, vol. No. 1:2025cv00542-Document 24 D.D.C. 2025.
[63] "Transportation Security Officer," *Transportation Security Administration*. Available: https://jobs.tsa.gov/tso-ssa. [Accessed: Jul. 01, 2025]



APPENDIX A. PCLOB REPORT RECOMMENDATIONS

The PCLOB report contained 13 recommendations in seven categories, including overall program; effectiveness and value; demographics and consequences of misidentification; transparency; individual participation; collection, sharing, retention, and use of data; and safeguards against misuse [1, p. 6-7]. AJL has highlighted six key recommendations that complement our own research into the lived experiences of the traveling public.

Transparency

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

➢ 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.

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.

APPENDIX B. GLOSSARY

1:1: "One to one" matching in the context of facial recognition technologies refers to ***facial verification***, which attempts to determine whether an image shows a particular person [11]. This is the type of matching that people use to unlock mobile phones, and that the TSA employs at standard opt-out checkpoints, where a live image of a traveler is compared to the photo on their identification document [1].

1:N: "One to many" matching in the context of facial recognition technologies refers to ***facial identificatio****n*, which attempts to answer the question, "Whose face is this?" [11]. Facial identification software can only look for matches within a gallery, or database, of photos or derived facial information. The TSA has introduced this type of matching at some airports and airlines as an opt-in program called "TSA PreCheck Touchless ID," where photos of travelers who have enrolled in TSA PreCheck who are scheduled to travel through an airport on a given day are added to a gallery for comparison with live photos of travelers at the checkpoint [1].

Biometric and Biographic: These are descriptions of data about people. Biometric data is derived from biological or physical aspects of a person. This can include fingerprints, faceprints, voice-prints, as well as data derived from the ways that people move, like walking gaits. Biographic data is information about a person's life, such as name, date of birth, travel history, and marital status. Both types of data can be used to identify people, and TSA uses both types of data at security checkpoints[1].

CAT, **CAT-1**, **CAT-2**: Credential Authentication Technology. These are devices that TSA officers use at security checkpoints for facial recognition, but they have other functions: Even if a traveler opts out of facial recognition, their identity document is scanned into a CAT device, which (1) attempts to determine whether the document is fraudulent and (2) displays biographic information about the traveler as well as the photograph of the traveler for the officer to perform manual identity verification. CAT-1 is the initial version of CAT devices. CAT-2 is the second generation of devices, and they are configured to perform facial recognition. They can be configured to perform 1:1 and 1:N matching. CAT devices are acquired by TSA from a France-based multinational corporation called IDEMIA Group under multimillion dollar contracts [1].

CBP: Customs and Border Patrol is a law enforcement agency housed under the Department of Homeland Security (DHS). At airports, CBP is concerned with customs (travelers entering the United States from other countries) while TSA is concerned specifically with aviation security. CBP has enforcement powers that TSA does not have. Both agencies use facial recognition technologies.

Demographic Differential: This term refers to different outcomes for different demographic populations. In the context of face recognition technologies, this refers to certain demographic groups having different accuracy rates, i.e. more or less false positives or false negatives compared to other demographic groups. This term is closely connected to the concept of "algorithmic bias."

Deployment: In the context of facial recognition, deployment is the process of turning the technology's underlying written code into a running, usable system. This activation occurs on physical hardware, which can range from cloud servers managed by corporations to locally owned servers or "edge" devices like CAT devices. A distinction is often made between "development" (the act of creating or modifying the software) and "deployment" (the act of launching and operating it. When people encounter and are processed by facial recognition, they are interacting with "a deployment," a specific version of the software's code running on particular hardware. Software deployments including changes to configurations can happen easily and remotely [60]. TSA has described changing CAT-2 devices' configurations to retain face data for longer during testing periods [1, p. 88].

DHS: Department of Homeland Security, a US federal executive department which has housed the Transportation Security Administration (TSA) since the DHS' creation in 2003 [8].

Faceprint: The digital representation of a face, wherein characteristics of a face are stored in a numerical format. This is similar in concept to a digital fingerprint, and is also referred to as a "template" [11]. When facial verification or facial identification is done through software, it involves comparing faceprints to each other to gauge similarity. Note that facial data can refer to the photograph or video ("live photo") from which the faceprint was derived and the faceprint. Deletion of facial data could refer only to the live photo, or to both the photograph and faceprint.

Facial Recognition: Used in everyday language to refer to technology that scans human faces to derive information including age, gender, race, and/or a person's identity. Used as a technical term by the biometrics industry to refer to the use of technology to analyze images of faces to verify if an individual matches credentials (facial verification/ 1:1 (one-to-one matching)) or if an image of a face matches a face in an existing database (facial identification/ 1:N (one-to-many matching). Some TSA communications use the term facial matching to refer to facial recognition.

False Negative: This refers to an error in facial recognition software. In 1:1 matching, or facial verification, this means that the software determined that two faceprints were not of the same person, when they actually were the same person. In 1:N matching, or facial identification, this means that a match was not made to any face in the gallery, even though it was present [1], [11].

False Positive: This refers to an error in facial recognition software. In 1:1 matching, or facial verification, this means that the software determined that two faceprints were of the same person, when they were actually two separate people. In 1:N matching, or facial identification, this means that a match was made to the wrong face in the gallery [1], [11].

FRTs: Facial Recognition Technologies. This refers to "a set of digital tools used to perform tasks on images or videos of human faces" which includes detection, attribute and emotion estimation, verification, and identification [11]. This report is mainly concerned with facial verification (1:1) and facial identification (1:N).

Gallery: The "set of people for whom an application has stored appearance information" [11]. In TSA's 1:N system, this may mean photographs of people scheduled to travel through an airport on a given day. A gallery often contains multiple images of each person associated.

Live Photo: TSA uses this term to refer to the photograph that is taken of travelers at TDC checkpoints by CAT-2 devices when facial recognition software is used. The "live photo" is used to create a "faceprint" or "template" which is then either compared to the photograph from the traveler's identification document (in 1:1 matching) or compared to all photographs in the gallery of travelers scheduled to travel through the airport on that day (1:N matching) [1].

PCLOB: Privacy and Civil Liberties Oversight Board, an agency within the Executive Branch. The board was established by the 9/11 Commission Act of 2007 with the mission of ensuring that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties, and can do this through oversight and advice. The board initiated an oversight project in 2019 on the use of facial recognition and biometric technologies in aviation security. A resulting report was published in May 2025 [1]. Designated as an independent agency, a full board is made up of five members. However, at the time of the report's publication, the board only had one member after three members were dismissed in January 2025 [1], [61]. After a court order, two board members were reinstated in May 2025 [62].

PIA: Privacy Impact Assessment, a document that government agencies are required to complete before developing or procuring information technology programs that implicate the privacy of the public by collecting, maintaining, or sharing identifiable personal information [1, p. 108]. PIAs are meant to be proactive, but PCLOB notes that DHS tends to wait until after systems have been deployed to publish PIAs for the systems [1, p. 108].

PreCheck: A "trusted traveler program" run by TSA ("TSA PreCheck" is a registered trademark of TSA) in which travelers go through an enrollment and threat assessment process that involves collecting traveler's biometrics and linking these to their biographic data. In exchange, TSA expedites screening for these travelers at security checkpoints. Travelers enrolled in PreCheck have

the option to opt in to 1:N face matching through “TSA PreCheck Touchless ID” at some airports with certain airlines [1].

Secure Flight: a TSA system which “matches the information individuals provide when booking their flight to, from, within, or over the United States to three subsets of the Terrorist Watchlist” [1]. Depending on the result, individuals may be issued a boarding pass and receive “enhanced screening, such as a pat down or explosives trace detection,” or not be issued a boarding pass and be prohibited from flying [1]. On the day of travel, information from Secure Flight is sent to CAT devices, which TSA officers use at TDC checkpoints [1].

SFPD: Secure Flight Passenger Data, the data sent from the Secure Flight system to CAT devices.

Template: Another word for “faceprint,” the digital numerical representation of a face. Sometimes also referred to as “biometric template.”

TDC: Travel Document Checker, the TSA airport checkpoint at which a traveler’s identity is confirmed for entry into the terminal. This includes “authenticat[ing] traveler identity documents, confirm[ing] that travelers match their presented identification, retriev[ing] prescreening status information for each traveler, and confirm[ing] that travelers have valid reservations for flights that day at that terminal” [1].

TSA: Transportation Security Administration, a government agency which is authorized 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” [1, p. 22]. The TSA is housed under the Department of Homeland Security (DHS).

TSO: Transportation Security Officer, a job position at the TSA. Along with SSA (Security Support Assistants), TSOs interact with travelers at security screening stations, operating CAT devices for face recognition or manual identity verification [63]. Travelers typically refer to TSOs and SSAs as “TSA Agents.”

TVS: Traveler Verification System, a cloud-based system operated by Customs and Border Control (CBP). The system compiles a gallery of photos of passengers who are scheduled to fly through an airport on a given day, and, when sent a live photo from a traveler, uses facial identification technology (1:N) to find a match for the traveler [1].

APPENDIX C. AJL SURVEY OVERVIEW

Survey Questions Used For Report

- Are you reporting an experience with the Transportation Security Administration (TSA)?* [Yes, this report is about the Transportation Security Administration (TSA - Domestic); No, this report is about Customs and Border Patrol (CBP - International); I'm not sure. I want to share my experience with both TSA and CBP]
- Notice*: Did you receive clear information about TSA's facial recognition program at the airport? [No, Yes]
- Signage*: Did you see signage about the right to opt out? [No, Yes]
- TSA Agent Ask*: Were you verbally informed of your right to opt out of the program? [No, Yes]
- Face Data: Do you want your airport face data held by the government? [No, Yes]
- Opt-out*: Did you verbally request to opt-out? [I was scanned before I had a chance to request to opt-out.I did not know opt-out was an option.I did not feel comfortable requesting to opt-out; I feared what consequences would follow.]
- Was your request to opt-out successful?* [Yes, I was able to successfully opt out; No, my face was still scanned although I opted out; Unclear.]
- Tell us what happened*
- Do you have any concerns about TSA's use of facial recognition?
- Where did you go through TSA screening?*
- Date of Flight*
- Select whom you authorize to share your story with* [With AJL Internal team only; With AJL and AJL's partners (like advocacy groups, legal firms, and journalists); Publicly. Share this story with the world.]

Demographic Information Gathered

- Gender identity:
- Racial identity:
- Please select your age [14-16; 17-20; 21-24; 25-28; 29-32; 33-36; 37-40; 41-48; 49-56; 57-64; 65-72; 73-120].

APPENDIX D. FULL LIST OF SURVEY AIRPORTS

Airport Name	Airport Code	Number of responses
Boston Logan International Airport	BOS	49
San Francisco International Airport	SFO	30
Denver International Airport	DEN	28
LaGuardia Airport	LGA	22
John F. Kennedy International Airport	JFK	19
Ronald Reagan Washington National Airport	DCA	16
Los Angeles International Airport	LAX	14
Hartsfield–Jackson Atlanta International Airport	ATL	10
Austin–Bergstrom International Airport	AUS	10
Newark Liberty International Airport	EWR	9
Orlando International Airport	MCO	9
Louis Armstrong New Orleans International Airport	MSY	8
Philadelphia International Airport	PHL	7
Seattle–Tacoma International Airport	SEA	7
Baltimore/Washington International Thurgood Marshall Airport	BWI	6
Cleveland Hopkins International Airport	CLE	6

Fort Lauderdale–Hollywood International Airport	FLL	6
Harry Reid International Airport	LAS	6
Chicago O'Hare International Airport	ORD	6
Phoenix Sky Harbor International Airport	PHX	6
Dallas Fort Worth International Airport	DFW	5
Salt Lake City International Airport	SLC	5
Albuquerque International Sunport	ABQ	4
Asheville Regional Airport	AVL	4
Nashville International Airport	BNA	4
Buffalo Niagara International Airport	BUF	4
John Glenn Columbus International Airport	CMH	4
Dallas Love Field	DAL	4
Daniel K. Inouye International Airport	HNL	4
Miami International Airport	MIA	4
Tampa International Airport	TPA	4
Hollywood Burbank Airport	BUR	3
Charleston International Airport	CHS	3
El Paso International Airport	ELP	3
Westchester County Airport	HPN	3

Washington Dulles International Airport	IAD	3
Oakland International Airport	OAK	3
Ontario International Airport	ONT	3
Portland International Airport	PDX	3
Pittsburgh International Airport	PIT	3
Raleigh–Durham International Airport	RDU	3
San Jose International Airport	SJC	3
Syracuse Hancock International Airport	SYC	3
California Redwood Coast – Humboldt County Airport	ACV	2
Cincinnati/Northern Kentucky International Airport	CVG	2
Gerald R. Ford International Airport	GRR	2
Greenville–Spartanburg International Airport	GVR	2
Indianapolis International Airport	IND	2
Ellison Onizuka Kona International Airport at Keahole	KOA	2
Long Beach	LGB	2
Chicago Midway International Airport	MDW	2
Minneapolis–Saint Paul International Airport	MSP	2

Kahului Airport	OGG	2
Palm Beach International Airport	PBI	2
St. Pete–Clearwater International Airport	PIE	2
Rhode Island T. F. Green International Airport	PVD	2
St. Louis Lambert International Airport	STL	2
Charles M. Schulz–Sonoma County Airport	STS	2
Tucson International Airport	TUS	2
Ted Stevens Anchorage International Airport	ANC	1
Bradley International Airport	BDL	1
Bangor International Airport	BGR	1
Bozeman Yellowstone International Airport	BZN	1
Charlotte Douglas International Airport	CLT	1
Detroit Metropolitan Airport	DTW	1
Eugene Airport	EUG	1
Fresno Yosemite International Airport	FAT	1
Huntsville International Airport	HSV	1
Mesa Gateway Airport	IWA	1
Jacksonville International Airport	JAX	1

Juneau International Airport	JNU	1
Lihue Airport	LIH	1
Manchester–Boston Regional Airport	MHT	1
Dane County Regional Airport	MSN	1
General Wayne A. Downing Peoria International Airport	PIA	1
Palm Springs International Airport	PSP	1
Richmond International Airport	RIC	1
Reno–Tahoe International Airport	RNO	1
Roanoke–Blacksburg Regional Airport	ROA	1
Frederick Douglass Greater Rochester International Airport	ROC	1
Southwest Florida International Airport	RSW	1
San Diego International Airport	SAN	1
San Antonio International Airport	SAT	1
Savannah/Hilton Head International Airport	SAV	1
Santa Barbara Municipal Airport	SBA	1
San Luis Obispo County Regional Airport	SBP	1
Orlando Sanford International Airport	SFB	1
Sacramento International Airport	SRQ	1

John Wayne Airport	SMF	1
Sarasota–Bradenton International Airport	SRQ	1
Yuma International Airport	YUM	1

APPENDIX E. TAGS FOR MANUAL DATA ANNOTATION

Each traveler response was manually tagged in four steps, each with a different category of tags. The tags were based on the open-ended questions that respondents could answer. Manual annotators did not view comprehensive information like traveler demographics, airport, or travel date, to avoid bias when tagging. Multiple tags from the same categories could be assigned to each response. If no open-ended question was answered, or if no tags fit, then no tags were assigned.

Step One: Opt-out Experience

Tag Name	Description
Unaware_OptOut_Possible	Didn't know opting out was an option.
Unaware_HowTo_OptOut	Wanted to opt out but didn't know how.
OptOut_Desired_but_NegativeConsequences Feared	Wanted to opt out but concerned something bad would happen
OptOut_Coerced_or_Discouraged	Pressured or discouraged by TSA Officer.
OptOut_Agent_Ignored_Refusal	Traveler refused facial recognition, but TSA Officer ignored the refusal.
OptOut_Camera_Exposure_PreLine	Traveler notes being in view of the camera while in line, before their turn.
NoChance_toOptOut	Traveler indicates their face was scanned before they knew what was happening
OptOut_Id_Scanned_Anyways	Traveler indicates that their face was scanned into the machine from their ID photo, whether or not the traveler opts out or not.
OptOut_Unclear_Outcome	Not sure if opt-out worked.
OptOut_Success	Opt-out was successful.
Traveler_Indicated_Was_Under_Time_Press ure	Rushing to catch flight / afraid of missing flight.

Traveler_Indicated_Financial_Pressure	Concerned about expenses they might incur from opting out.
Traveler_Indicated_Length_Of_Line	Noted long line / not wanting to inconvenience others.
Signage_Missing	No signage seen.
Signage_Difficult	Signage seen but likely missed by others.
Signage_Clear	Signage was clear.
Signage_Incomplete	Saw sign but link/data was impractical.

Step Two: Traveler Treatment

Tag Name	Description
Treatment_Shame_Speech	TSA officer made rude or shaming remarks.
Treatment_Shame_BodyLanguage	TSA officer used hostile body language (e.g. eye rolling.
Treatment_Shame_PublicCallout	TSA officer called them out or made an example of them.
Treatment_Shame_LineDelayAccusation	TSA officer accused them of slowing down the line.
Treatment_Shame_ComparisonToCompanion	TSA officer treated them worse than travel companion
Treatment_Dignity_RespectfulSpeech	TSA officer respectfully acknowledged opt-out verbally.
Treatment_Dignity_PositiveBodyLanguage	TSA officer used positive gestures (smile, wave-through.
Treatment_Dismissal_TooLate	TSA officer said it was too late to opt out.
Treatment_Dismissal_CamerasEverywhere	TSA officer said other cameras are always recording.

Treatment_Dismissal_OptOutUseless	TSA officer implied opt-out was meaningless.
Treatment_SentAsideForManualCheck	Traveler was sent aside for further manual check.
Treatment_SecurityScreeningDelayLinkedToOptOut	Traveler believes extra screening was due to opting out.
Treatment_Provided_Incorrect_information	TSA officer provided traveler with incorrect information, like that the program is mandatory.

Step Three: Concerns

Tag Name	Description
Concerns_GeneralPrivacy	Indicated general concerns over privacy.
Concerns_LackOfInformedConsent	Lack of informed consent.
Concerns_LackOfOptOutKnowledge	Didn’t know how/if to opt out.
Concerns_LackOfDataPrivacyKnowledge	Didn’t understand privacy practices.
Concerns_DataBreachesOrInsecurity"	Worried about data breaches/security.
Concerns_DataSharingWithOtherParties	Concern about data being shared with other parties.
Concerns_OpaqueDataStorage	Data storage felt hidden/unclear.
Concerns_DistrustDataDeleted	Doesn't trust that data will be deleted.
Concerns_CivilRightsViolations	Civil rights risks/concerns.
Concerns_BiasedOrDiscriminatorySystems	Concerned about bias/discrimination.
Concerns_NegativeConsequencesForOptingOut	Worried about negative consequences for opting out.

Concerns_SurveillanceOrAuthoritarianism	Concerned about surveillance/power.
Concerns_LawEnforcementBorderControl	Data use by law enforcement/border.
Concerns_TechnicalSystemInaccuracy	Concerns about technical system's accuracy.
Concerns_MakesVerificationSlower	Facial recognition process slows down ID verification process.
Concerned_ChildrenScanned	Worried about children being scanned.
Concerns_Unnessecary	Questions whether or notes that facial recognition is unnecessary; should not be used at all.

Step Four: Benefits

Tag Name	Description
Benefit_SufficientInformation	Had enough information about the program.
Benefit_SecurityEnhanced	Made process faster.
Benefit_LowDataRiskPerceived	Didn't feel data was at risk.
Benefit_GovtHasDataAnyway	The government already has data; didn't matter.
Benefit_SystemNeutral	System felt neutral/unbiased.
Benefit_NoOptOutPenalty	No harm in opting out.
Benefit_DataUseLimited	Believes data only used at checkpoint.
Benefit_AccurateTechnology	Technology seemed accurate.

www.ajl.org