Privacy in practice: Facial recognition technology at United States airports

Niharika Tomar
University of Wisconsin–Madison
Madison, WI
ntomar@wisc.edu

Sophie Stephenson
University of Wisconsin–Madison
Madison, WI
srstephenso2@wisc.edu

Zhonggang Li
University of Wisconsin–Madison
Madison, WI
zli769@wisc.edu

ABSTRACT

Facial recognition technology (FRT) has become more and more widely used over the past few years. In this work, we focus on one recent implementation of FRT: traveler identification during air travel. The use of FRT in air travel presents the potential for privacy violations and surveillance, since it collects biometric data and often is operated by government agencies; thus, any implementation must carefully address related privacy concerns. Through a survey of travelers and an analysis of current FRT implementations in U.S. airports, we reveal that currently implemented FRT systems pose a significant privacy violation for travelers. The systems do not effectively protect travelers' private data, and further, airlines and border agencies do not effectively acquire the consent of travelers before applying FRT. Our study provides insights regarding privacy issues in U.S. airports and the privacy concerns of FRT that should be addressed in future.

Author Keywords

Facial recognition technology; border control; privacy.

INTRODUCTION

Facial recognition technology (FRT), once used for secret authentication and investigation, has now found its way to the masses. From airports to shopping centers, law enforcement agencies, social media platforms, and even the White House, FRT can be seen at work. Although having many potential benefits like being able to solve/prevent crimes, recognize individuals for faster and secure clearance and also reduce manual human labor to check and correct security behaviors, FRT is also highly controversial. It has caused many to raise concerns about the accuracy and ingrained bias of these algorithms, and more fundamentally, how it threatens the right to one's privacy.

With this in mind, we turn our attention to one up-and-coming use for FRT: border verification. *Automated border control (ABC)* systems use FRT along with fingerprints and iris scanning to verify travelers more efficiently and accurately than was previously possible. These systems are quite useful, but have the same potential privacy issues as FRT, if not more.

Figure 1. A traveler uses FRT at an airport in Boston. Source: wbur.org/bostonomix/2017/06/21/jetblue-facial-recognition-pilot.

As ABC is a relatively new concept, there is a lack of prior work on the subject. Though researchers have studied how travelers perceive these systems, they have mainly focused on the EU, and most attempted to gauge interest in ABC rather than asking about travelers' actual experiences with it. Prior work has raised several privacy concerns of ABC, and some have proposed guidelines for how to design systems which better preserve privacy; however, it is unknown whether current ABC systems were designed with these guidelines in mind. Finally, ABC was originally only available to a small number of pre-enrolled travelers, and only recently has it become more widely accessible. As a result, the role of active consent in ABC has not been sufficiently studied.

We aim to better understand the extent to which current facial recognition systems at the United States border respect the privacy and consent of travelers. To achieve this, we investigate the following aims:

R1: To what extent do participating US airlines seek active consent in the use of facial recognition for ABC?

R2: To what extent are current ABC systems in the US built in a privacy-preserving manner?

It is our hope that in answering these questions, we can better understand the role of privacy and consent in today's ABC systems.

CS770 Spring '21, January 26–May 3, 2021, Madison, WI, USA

ACM ISBN 978-1-4503-2138-9…$15.00

DOI: https://doi.org/10.1145/3313831.XXXXXXX

RELATED WORK

Ethical issues of FRT

After the 9/11 terrorist attacks on the United States, there has been demand to apply powerful tools to guarantee national security. Video surveillance and facial recognition technology are becoming the subject of interest to aid public security [5, 7]. On the other hand, facial recognition technology is also becoming a threat to invasion of privacy [8, 28].

Facial recognition technology, being highly evolved in its identification accuracy, causes several ethical issues [6, 34]. One dilemma in facial recognition is the potential for gender discrimination [17]. Many techniques are used in gender recognition; however, transgender individuals have overwhelmingly negative attitudes towards this system. How to properly use gender recognition in practice is a problem still in debate. The other big issue is the potential for race discrimination by using facial recognition technology. The current commercial facial recognition technology is biased across different racial groups [38], which may be misused to target certain people in multiracial society. Thirdly, the application of facial recognition technique to distinguish undocumented immigrants is also regarded as a risk to privacy [15]. Finally, the authority of facial recognition technology to be used in law enforcement departments is also in debate. Although more than half people trust law enforcement to use this technique to improve safety [35], there are some concerns about excessive governmental power and invasion of human rights.

Privacy-preserving facial recognition prototypes

The widespread use of face recognition system raises privacy risks since the biometric information may be collected and misused to profile individuals against their will [25]. This raises the desire to construct privacy-preserving face recognition systems [4].

One way to preserve privacy is to use a client-server interface, and the server is responsible for face image storage and processing without revealing any useful information to the server [36]. Another strategy is to encrypt the face images. The face images are typically encrypted and processed as Eigenface to ensure privacy preservation [32, 39]. This approach, however, requires a large amount of operations and on-line communication and is computationally expensive. These restrictions make this proposal hard to be deployed in practical large-scale applications.

In recent years, alternative strategies have been developed to provide privacy-preserving. Using binary feature vectors is proposed to protect privacy in a helper data system to replace Eigenface [21]. Using binary features can significantly increase data communication efficiency although it sacrifices the classification and identification accuracy. In a recent study, the author proposed a privacy-friendly alternative for large scale facial recognition. Instead of running facial recognition software on all video data, they automatically extract a high quality snapshot of each detected person without revealing their identity. This snapshot was encrypted and access to these snapshot was only granted after legal authorization. The snapshot was then selected by a unsupervised face image quality assessment and for identification [26].

Another privacy risk exists in the scenario when sharing photos online [18]. FoggySight is proposed as a solution that uses a community protection strategy to protect privacy in online sharing system. It applies lessons learned from the adversarial examples literature to modify facial photos in a privacy-preserving manner before photo images are uploaded to social media [19].

Facial recognition at the border

Despite the ethical issues of facial recognition, one place it has become prevalent is in border control. Automated border control systems combine live biometric samples and previously verified data, such as from an e-Passport, to automatically verify travelers and ensure the validity of their documentation [22]. These systems commonly use facial recognition as the default biometric component since it is the most socially acceptable, interoperable, and non-intrusive option [20, 22, 23]. With passenger traffic constantly increasing (the current pandemic notwithstanding), ABC systems can ease the burden of border guards, more accurately verify travelers, and provide a more seamless border-crossing experience [1, 22]. ABC systems could also offer a more socially-distant, touchless option for a post-pandemic world [16].

Privacy issues regarding facial recognition are no less pressing in a border control context. For ABC systems, the primary privacy concern is the potential for *function creep*. This occurs when stored biometric data is exploited for a purpose other than the one originally agreed to by stakeholders [20, 27, 37]. At the border, one way that function creep can occur is if legal authorities are granted access to stored biometric data [37]. Unfortunately, this has already happened at least once, when EU law enforcement agencies were given access to the EURODAC fingerprint database originally meant for asylum applications [2]. Further, the fact that ABC systems are used in the interest of national security may complicate the legal basis for privacy protection. For example, the EU's General Data Protection Regulation (GDPR) has certain legal loopholes which allow for proportional privacy violations in the interest of national security [2]. As a result, EU border agents may be entitled to use biometric data without informed consent from travelers and without being transparent about how the data is used [1].

Researchers have proposed methods for creating more privacy-preserving ABC systems. To prevent function creep, for example, biometric data stored in ABC systems should be (a) minimal, containing only the data needed for verification; (b) unlinkable with data from other biometric databases; (c) revokable by the owner of the data; and (d) irreversible in that the stored data does not reveal the identity of the person whose data it is [27, 37]. Additionally, Tsormpatzoudi et al. argued that ABC would benefit from a privacy by design strategy, where techniques such as automated data erasure are built into the design from the start [37]. Though these guidelines are valuable for designing future ABC systems, to our knowledge, no studies have investigated whether these privacy-preserving steps are implemented in current ABC systems.

Unsurprisingly, travelers have privacy concerns about ABC systems. Abomhara et al. found that at Romanian borders, nearly half of the travelers surveyed were worried about potential unauthorized disclosure of their data and feared that their privacy would be violated [1]. In Norway, a survey of over 6000 travelers found that while a large proportion were interested in automated options at the border, only 15% were interested in biometric options [16]. However, there is evidence that travelers are willing to use ABC systems despite these concerns. Negri et al. showed that 83% of travelers surveyed in Brazil would use biometric technology at airports [31]. In the United States, Morosan found that though people with privacy concerns are less willing to disclose their biometric information, they can be swayed to do so if the benefits are clear and they feel the ABC environment is secure [30]. Morosan in a subsequent study reiterated that privacy concerns are not a strong factor in whether American travelers would use ABC systems [29].

METHODS

Traveler survey

Prior studies have investigated traveler perceptions of ABC. However, few studies have been performed in the US, and those that were focused on travelers' interest level in ABC rather than their experiences with it. Additionally, there is a lack of investigation into whether ABC systems are being used with the full consent of travelers crossing the border. Therefore, we ask: to what extent do US implementations of ABC seek informed consent for the use of FRT from participating travelers? We explore this questions using a survey.

Study setting & population

Our population of interest is travelers who have used FRT (or opted out of using FRT) to verify their identity while traveling. We chose to include both participants who have used ABC systems and participants who have used FRT during other parts of the airport process—we hoped that this would increase the amount of data we were able to collect in a short time frame. We would prefer to survey travelers in person at an international airport, but due to budget and time constraints and the ongoing pandemic, we performed our study online. Demographic information for our participants is shown in Fig. 2.

Data collection

We used a self-selected survey to study this question. We advertised the survey on social media, email lists, travel channels, and survey threads on Reddit over a period of two to three weeks. The exact platforms used were: r/samplesize, r/takemysurvey, r/grouptravel, r/solotravel (Reddit survey threads and travel channels), The Research Survey Exchange Group on Facebook, our class (CS770 HCI) Piazza group, and our respective roommates, friends, fellow students and family members who have experienced air travel at least once in their life.

Materials & instruments

Our survey was created using Qualtrics. The survey consists of several sections:

- **Filtering.** We asked the participant's age, whether they have ever used FRT at US airports, and whether they have ever opted out of using FRT at US airports. We terminate the survey if the participant is under 18, and we skip to the demographics section at the end if the participant has not used FRT or opted out of using FRT at US airports.
- **Usage information.** We gather information about the participant's experience using FRT. We use multiple-choice questions to ask in which scenario they used FRT (e.g., at check-in or at border control), the location(s) where it was used, how far in advance they were aware of the use of FRT on their trip, and whether, to the participant's knowledge, the use of FRT was required. We used the Ban Facial Recognition Map[1] to compile the list of possible locations.
- **Likert scales.** We ask participants to rank their level of agreement (strongly agree, somewhat agree, neither agree nor disagree, somewhat disagree, or strongly disagree) to a series of statements regarding attitudes on FRT, biometrics, ABC, privacy, and consent.
- **Free response.** We ask participants to indicate whether they would prefer to use facial recognition, another biometric, or manual methods to verify their identity at airports. We ask them to explain their answer with free text.
- **Demographics.** We ask for participants' travel habits, including frequency of travel on an airplane, the year most recently traveled on an airplane, and frequency of travel across the US border. The survey ends with collection of participant demographic information: gender, ethnicity, and education level.

Before running the survey, we piloted it with fellow students and a few volunteers to see how it can be improved.

Data cleaning & filtering

We gathered 30 responses total. Of these, nine were incomplete. We analyzed the remaining 21 responses for inconsistencies and found none.

Data analysis

We first analyzed the quantitative data. We gathered some descriptive statistics to get a sense of the basic findings. Because our survey was exploratory and not meant as an experiment, we did not perform any inferential statistics.

Then, we used coding to analyze the free-response questions. Because of the small amount of data (12 qualitative responses total), one author coded the responses and developed code categories. In total, there were 13 codes and 3 categories.

Evaluation of the privacy-preserving property of different facial recognition systems implemented by ABC

In this section, we conducted a privacy impact assessment for different facial recognition technologies used by ABC. We focused on a categorical analysis. We included a technical analysis of different facial recognition systems used in US ABC.

[1] https://www.banfacialrecognition.com/map/

Research Question

Our goal was to compare the current implementations of facial recognition technology used by US border control and evaluate the extent to which they preserve subjects' privacy.

Study Setting And Population

The facial recognition systems used by two major agencies, *US Customers and Border Protection* (CBP) and *Transportation Security Administration* (TSA), will be our research targets. The systems include but are not limited to air, land, and sea ports of entry. The passengers who use the ABC systems and are subject to the utilization of facial recognition were our study population.

Data Collection Methods

To address our objective, we reviewed the documents which list the requirements of CBP and TSA about the privacy protecting terms released to public. Moreover, we collected any public report about the events of privacy leak from facial recognition technologies used by US ABC. We also compared the technical parameters and characteristics of the different facial recognition systems. We address the privacy issues in four key stages of facial recognition:

- **Enrollment** During the enrollment stage, the facial recognition system obtains the image from passenger. This stage has a relatively minor effect on privacy, but may be conducted without passengers' approval. We collected data to confirm the existence of an approval notice and its clearance from different facial recognition systems used in CBP and TSA.
- **Storage** The collected image data is stored in either a local or remote server for future analysis. This is the most likely stage for privacy leakage. We compared the techniques used by CBP and TSA in their data storage. The events of privacy leakage published by media were be recorded.
- **Database access** The facial recognition system will need to get access to remote database for criminal or banned face images for safety identification. This is another risky part of potential privacy leakage. The access to this database should be granted in a proper way. We will assess and compare the current access authority from different facial recognition systems. Some novel techniques, which restrict the misuse of the national criminal database, are also listed and analysed in our study.
- **Matching** Multiple matching algorithms are applied in current implemented facial recognition systems. They usually have a trade-off of accuracy with privacy preservation. The advantage and disadvantages of these technologies are thoroughly analyzed in our study.

Data Analysis Approaches

We analyzed and calculated the frequency of privacy leaks for each facial recognition system. Public concerns about each system were included as an important factor. We summarized the techniques used for each facial recognition system in a table and thoroughly compared and analyzed their pros and cons.

As discussed in data collection section, the data collected from the four stages of using facial recognition was our analysis focus. Different types of privacy risks will be discussed for our selected facial recognition systems. These risks will include the following terms.

- **Information Leakage Assessment** We used the data collected from the storage and acquisition stages in this assessment. We reported the privacy leakage incidence occurred in FRT.
- **Technical Parameter Analysis** This is an analysis in the perspective of technique. We evaluated the difficulties of deciphering the matching images in this analysis. The data storage and collection policies will be reported in our study.

RESULTS

Traveler survey

We performed a traveler survey to understand travelers' experiences with FRT at airports. We obtained 21 valid responses to our survey. Twelve participants had used FRT at a US airport, while nine had no experience with FRT at US airports. None of our participants had opted out of using FRT at US airports. A summary of participant demographics can be found in Fig. 2. Traveler responses to Likert scales are shown in Fig. 3. In our analysis, "Strongly agree" correlates to a score of 1, while "Strongly disagree" correlates to a score of 5.

Traveler preferences

We asked participants who had used FRT which method of identification they would prefer to use at the airport in the future: facial recognition, another biometric (e.g., fingerprints) or manual verification. Half of these participants (6/12) would prefer to use manual methods, 25% (3/12) would prefer another biometric, and 25% would prefer to use FRT. Participants' reasons for choosing each method fall into two categories: privacy concerns and characteristics of FRT (positive and negative).

FRT. Of those who would prefer to use FRT in the future, two discuss its efficiency and ease of use. However, two also mention drawbacks. P5 (gender=M, age=45-54) posits, "Tech exists to improve the user experience and security. However it should be used in a secure and transparent way. Ideally users would be given a choice." P18 (F,25-34) also brings up the issue of bias: "I am not too worried about reprocutions as a white citizen of USA, but I can see how others would choose not to use it." Even those who are comfortable using FRT see the possible drawbacks of its use.

Other biometrics. Of the three participants who would choose to use another biometric, reasons are varied. One mentions the functionality issues of FRT compared to other biometrics: "Faces change, fingerprints don't" (P8: F,25-34). Another, P14 (M,18-24) is concerned about privacy and consent issues with FRT:

> I think that facial recognition software could be used for ethically questionable purposes in the present or near future (i.e. tracking someone's location without their knowledge or consent) and the more it's normalized, the sooner that future will come.

Demographic item	N	%
Total	22	
Age		
18-24	12	54.6
25-34	5	22.7
35-44	2	9.1
45-54	3	13.6
Gender		
Female	14	63.6
Male	8	36.4
Non-binary / third gender	0	0.0
Ethnicity		
White	16	76.2
Black or African American	0	0.0
American Indian or Alaska Native	0	0.0
Asian	5	23.8
Native Hawaiian or Pacific Islander	0	0.0
Latinx	1	4.8
Other	2	9.5
Highest education level		
High school diploma	0	0.0
Some college	6	23.7
2 year degree	3	9.1
4 year degree	9	40.9
Professional degree	4	18.2
Doctorate	1	4.6
Rate of air travel pre-2020		
Never	0	0.0
Very rarely	3	13.6
Once every few years	2	9.1
1-2 times a year	11	50.0
3-8 times a year	6	27.3
Once a month	0	0.0
Year most recently traveled by air		
2021	3	13.6
2020	7	31.8
2019	5	22.7
2018	4	18.2
2017 or earlier	3	13.6
Rate of US border crossing pre-2020		
Never	3	13.6
Very rarely	8	36.4
Once every few years	4	18.2
Once a year	5	22.7
Multiple times a year	2	9.1

Figure 2. Summary of participant demographics.

Manual methods. These concerns about privacy are echoed by those who would prefer to use manual methods. Some (4) are concerned about any use of biometrics or collection of personal data. Additionally, one participant notes specific concerns with trust and the US government: “I do not want biometrics used in any way. I do not trust any entity to store my personal data. Especially not the us government" P12 (M,25-34). Further, some participants mention specific characteristics of FRT. P1 (F,18-24) is concerned that face recognition is not more accurate then manual verification, and further that face biometrics are not kept secret. She expresses, “I also don’t think faces are necessaril[y] ’sensitive information’ - people post their faces online all the time already." One participant (P4: F,18-24) mentions that there is no need for it: “I don’t see the need for facial recognition to be used. It’s an invasion of privacy." Clearly, privacy is a concern for many passengers; this only increases the need for airlines to seek informed consent and offer the option to opt out.

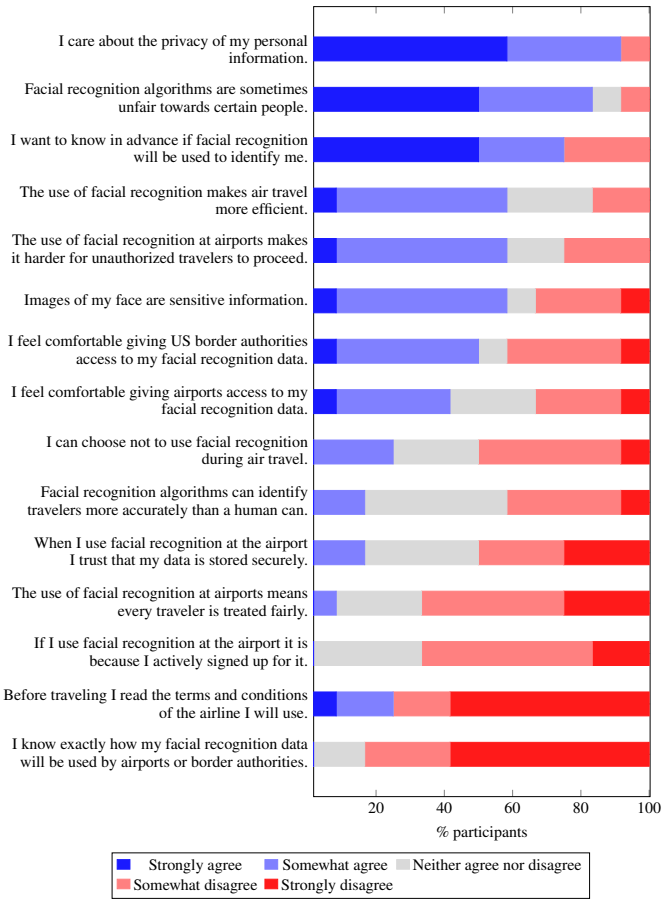

Figure 3. Participant responses to Likert scales.

Consenting to FRT

Unfortunately, our results showed that in many cases, airports do not properly seek the informed consent of travelers to use FRT for identification. Informed consent can only be given when the traveler has full and correct knowledge of the consequences of using FRT, has time to come to an informed decision, and is able to opt out if desired. The traveler experiences we collected show airports are deficient in all of these aspects of informed consent.

Transparency. None of our participants agreed they knew exactly how their FRT data would be used by airports ($M = 4.42, SD = 0.76$). This may in part be due to the fact that, unsurprisingly, most travelers disagreed that they read the airport terms and conditions before travel ($M = 4.00, SD = 1.41$). This indicates airports do not properly inform travelers about the usage of their data. Even if that information is included in the terms and conditions, it needs to be more readily available or that information will not reach travelers. Additionally, participants also did not on average agree that airports would safely store their FRT data ($M = 3.58, SD = 1.04$), indicating a lack of trust in the security of their data.

Ability to prepare. Most participants want to know beforehand if facial recognition will be used to identify them ($M = 2.00, SD = 1.22$). However, the majority (9/12) were

Figure 4. Airports where CBP has implemented FRT for border control. [10].

only aware FRT would be used just before they had to use it. This lack of awareness means travelers do not have time to make a proper decision on whether to use FRT, especially in a stressful airport environment.

Ability to opt out. Though airports claim to offer travelers a right-to-deny, over half of our participants who had used FRT (7/12) thought that the use of FRT was required at some point during the process. A majority of participants also disagreed that they could choose not to use FRT during air travel ($M = 3.33, SD = 0.94$). This is a critical issue. Regardless of whether travelers actually have the ability to opt out, this ability is meaningless unless travelers are *aware* that they can opt out.

FRT Implementations in US Airports

CBP started pilot tests of their implementation of facial recognition system in 6 airports in 2018. At the end 2020, 27 U.S. airports had deployed facial recognition technology for travelers who exit the U.S. and 18 airports had deployed it for travelers who enter the U.S (Figure. 4). It is expected that by the end of 2021, the top 20 major airports in U.S. will have implemented FRT systems for international travelers [24]. As of 2020, over two million travelers on over 15,000 flights have used FRT on their exit. This number is expected to further explode to 16,300 flights per week [12].

Privacy Principles And Policies for ABC

The *Fair Information Practice Principles* (FIPP) are internationally recognized voluntary principles for privacy. They were first proposed for protecting the privacy and security of personal information in the United States in 1973 by a U.S. government advisory committee. The FIPP served as the basis for the Privacy Act of 1974, which governs the collection, maintenance, use, and dissemination of personal information by federal agencies [33]. Also, the E-Government Act of 2002 requires related agencies to conduct Privacy Impact Assessments (PIA) that analyze how personal information is collected, stored, shared, and managed in a federal system. All regulations and instructions conducted by FRT system in U.S. airports should follow.

Current FRT contains a compilation of following security guidance for its implementation: (1) management controls, focused on managing system information security controls and system risk; (2) operational controls, meant to improve the security of particular systems; (3) technical controls, which provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data; and (4) privacy controls, which protect and ensure the proper handling of passenger privacy.

Current FRT Used in ABC Systems

CBP-implemented FRT. CBP has developed and implemented a Traveler Verification System (TVS) to serve as the major facial recognition matching service for the Biometric Entry-Exit Program.

TVS is a cloud-based biometric matching technique that uses an algorithm to compare live photos with the existing photos stored in a remote database. It can be performed in both 1:N or 1:1 facial recognition matching. In air and sea environments, CBP receives travelers' biographic information in advance of travel through passenger manifests submitted by commercial and private aircraft operators and commercial sea carriers. TVS then searches Department of Homeland Security (DHS) databases of photos associated with travelers listed on the manifest and creates a pre-staged "gallery" of templates created from those photos.

Beside 1:N matching, TVS allows for 1:1 matching. For 1:1 matching, TVS compares a live photo of a traveler against another photo of that traveler, such as from a passport photo or VISA photo. This type of matching can be used when CBP does not have passenger manifest information and cannot create a gallery in advance or does not have an existing photo available for matching. These two matching strategies work together to ensure efficient facial recognition in different scenario and for different customers by CBP in daily tasks [13] (Figure. 5).

As shown in Figure. 6, TVS uses pre-obtained photos from DHS databases to generate a gallery. This ensures faster matching efficiency onsite. To be in accordance with the privacy protection policy, TVS allows U.S. citizens and other exempt travelers to opt out of facial recognition identification, and the CBP may grant such requests on a case-by-case basis. However, the policy of notifying travelers and criteria for granting exemptions have never been clarified in their website or airport guidelines.

TSA-implemented FRT. At the travel document checker position, TSA officers manually verify travelers' identities by comparing travelers faces to the photos on their travel identification documents. The current facial recognition technique for TSA is still not decided. But in 2018, the TSA published its Biometrics Roadmap,[3] which proposed its plan to partner with CBP and use their current TVS system. TVS usage by TSA mainly focuses on two groups of travellers, international travelers and TSA Pre-Check travelers. The expansion of FRT to domestic travelers is still under debate and needs to be approved by administration.

Newly implemented FRT. On October 29, 2020, CBP officials announced an implementation of a facial-recognition

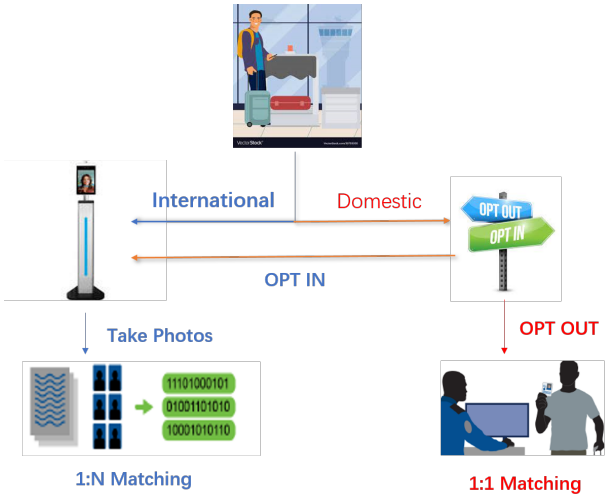

Figure 5. The TVS system used by CBP has two algorithms, 1:1 matching and 1:N matching. Compared to international travelers, domestic travelers have the option to opt out and choose 1:1 matching to avoid automatic facial recognition and wait for CBP officer to scan photos from travel documents for 1:1 matching. Figure is adapted and modified based on [13].

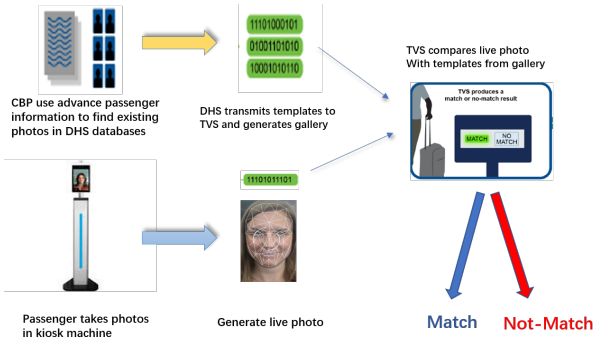

Figure 6. The TVS system uses advanced passenger information to find existing photos of travelers in DHS database. Passengers take live photos a kiosk, and these photos will be matched with the gallery of pre-obtained photos. Figure is adapted and modified based on [13].

process at Los Angeles International Airport (LAX). This new process will screen passengers entering the country. The newly implemented process is called Simplified Arrival, which uses FRT to automate the manual document checks that are already required for admission into the U.S. In Simplified Arrival, an arriving passenger walks up to the CBP booth, has their picture taken, and within seconds, the system is able to identify them and compare the pictures to images in Department of Homeland Security databases. Passengers will then walk to the Global Entry kiosks to verify their photo, hand a receipt to the CBP officer and exit the airport (Figure 7).

Travelers who want to opt out of Simplified Arrival may notify a CBP officer as they approach the primary inspection point. These travelers are required to present a valid travel document for inspection by a CBP officer, and they are processed consistent with existing requirements for admission into the U.S. Until now, three airports in California—LAX, SFO and SJC—are currently applying Simplified Arrival as their facial

Figure 7. Facial recognition gate in LAX [14].This new technology gate with FRT can board 350 passengers in 20 minutes.

recognition technique to enhance border control efficiency[9]. More international airports are considering Simplified Arrival in the future.

Compared to previous versions of TVS (such as the pilot TVS system 2019), Simplified Arrival pays more attention to cybersecurity. For instance, new photos of US citizens in Simplified Arrival system are deleted within 12 hours. Photos of most foreign nationals are stored in a secure Department of Homeland Security (DHS) system remotely to address privacy concerns.

Reports of Privacy Leakage

In May 2019, a US CBP subcontractor discovered it had been the victim of a cyber attack. Subsequently, some CBP data, including traveler images from CBP's facial recognition pilot, appeared on the dark web. In the official report released by DHS [11], this incident may have caused approximately 184,000 traveler images from CBP's facial recognition pilot study to be leaked. Further survey found at least 19 of the images were posted to the dark web.

This incident was found to be caused by an unauthorized access and improper storage of the image data. The survey revealed that Perceptics,[2] a high-performance imaging company, gained unauthorized access to CBP's data through cameras located at the test site in Anzalduas, TX. Perceptics subsequently admitted that it had downloaded approximately 184,000 traveler images from the equipment in conjunction with the work order tickets. The data was hacked due to an unencrypted hard drive in their local office.

This incident highlights the need for proper maintenance and storage of images obtained through FRT in airport. CBP added annual training and inspection to ensure travelers' privacy and avoid such incidents; however, we must still be wary that events like this may occur in the future.

DISCUSSION

Throughout this paper, we aimed to better understand the extent to which current facial recognition systems in airports respect the privacy and consent of travelers. We explored this research question through a survey of travelers who have used FRT and through an analysis of current implementations.

[2]www.perceptics.com

For current implementations, TVS presents an opportunity for function creep. Because TVS uses facial images from a variety of sources, both public and private, there is always a risk that the airline or airport will use the biometric data for a purpose other than identity verification, such as for commercial or marketing purposes. Several policies could mitigate this risk. For instance, CBP is required to provide notice before sharing the TVS images with other law enforce agents, such as immigration or counter-terrorism agencies. For airlines, stored photos should be deleted and removed within twelve hours to prevent function creep. However, these policies and roles can't efficiently rule out the risk of a breach.

Moreover, airports do not properly seek the informed consent of travelers to use FRT for identification. With the aforementioned privacy concerns, it is vital that travelers are given a choice to opt out of this technology. Unfortunately, as we saw in our traveler survey, travelers still often believe the use of FRT is required. Even if they are aware of the ability to opt out, travelers do not have enough time or information about the system to make an informed decision on whether to opt out. This is an urgent issue. We must improve the security of facial images collected by FRT and push airlines and border agents to *actively* seek truly informed consent from travelers.

Limitations

Our study is most limited by the number and diversity of the participants in our traveler survey. We were only able to collect a small number of participants due to time and budget constraints, and these participants are quite homogeneous (mostly made up of our peers). Additionally, many documents containing information about currently-implemented ABC technology are not available to the public.

CONCLUSION

In this paper, we investigated the use of FRT at US airports to better understand the extent to which these current facial recognition systems respect the privacy and consent of travelers. We explored to what extent participating US airlines seek active consent in the use of facial recognition for ABCs and to what extent the current ABC systems in the US are built in a privacy-preserving manner. We found that in addition to not seeking the informed consent of travelers, airports implement FRT with critical privacy holes. If the use of FRT at airports is to be ethical, future work must be done to address these pressing issues of consent and privacy.

REFERENCES

[1] Mohamed Abomhara, Sule Yildirim Yayilgan, Livinus Obiora Nweke, and Zoltán Székely. 2021. A comparison of primary stakeholders' views on the deployment of biometric technologies in border management: Case study of SMart mobILity at the European land borders. *Technology in Society* 64 (2021), 101484. DOI:http://dx.doi.org/https://doi.org/10.1016/j.techsoc.2020.101484

[2] Mohamed Abomhara, Sule Yildirim Yayilgan, Marina Shalaginova, and Zoltán Székely. 2020. *Border Control and Use of Biometrics: Reasons Why the Right to Privacy Can Not Be Absolute*. Springer International Publishing, Cham, 259–271. DOI: http://dx.doi.org/10.1007/978-3-030-42504-3_17

[3] US Transportation Security Administration. 2018. "TSA BIOMETRICS ROADMAP". (2018). https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf

[4] Thomas Schneider Ahmad-Reza Sadeghi and Immo Wehrenberg. 2009. *Efficient Privacy-Preserving Face Recognition*. Springer International Publishing, 229–231. https://link.springer.com/chapter/10.1007/978-3-642-14423-3_16

[5] Ian Berle. 2020a. *Privacy and Surveillance Surveyed*. Springer International Publishing, Cham, 39–56. DOI: http://dx.doi.org/10.1007/978-3-030-36887-6_4

[6] Ian Berle. 2020b. *Some Ethical and Legal Issues of FRT*. Springer International Publishing, Cham, 27–38. DOI: http://dx.doi.org/10.1007/978-3-030-36887-6_3

[7] Kevin Bowyer. 2004. Face recognition technology: security versus privacy. *IEEE Technology and Society Magazine* (2004). DOI: http://dx.doi.org/10.1109/MTAS.2004.1273467

[8] Andrea Cavailaro. 2007. Privacy in Video Surveillance [In the Spotlight]. *IEEE Signal Processing Magazine* 24, 2 (2007), 168–166. DOI: http://dx.doi.org/10.1109/MSP.2007.323270

[9] CBP. CBP Introduces Simplified Arrival at SFO and SJC. (????).

[10] CBP. 2017. "Map of the U.S. International Airports and Legacy U.S. Customs and Border Protection (CBP) Model Ports Program Airports in the United States". (2017). https://commons.wikimedia.org/wiki/File:Figure_2-_Map_of_the_17_Busiest_U.S._International_Airports_and_Legacy_U.S._Customs_and_Border_Protection_(CBP)_Model_Ports_Program_Airports_in_the_United_States_(34183472493).jpg

[11] DHS. 2010. "Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot". *DHS* (2010). https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf

[12] Geoffrey A. Fowler. 2019. "Don't smile for surveillance: Why airport face scans are a privacy trap". *The Washington Post* (2019). https://www.washingtonpost.com/technology/2019/06/10/your-face-is-now-your-boarding-pass-thats-problem/

[13] GAO. 2020. facial recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues. *Gorvenment Report* (2020). https://www.gao.gov/products/gao-20-568

[14] Hillary Grigonis. 2018. Board 350 passengers in 20 minutes? Facial recognition passes testing at LAX. (2018). https://www.digitaltrends.com/photography/lufthansa-self-boarding-gates-biometrics/

[15] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. *Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants*. Association for Computing Machinery, New York, NY, USA, 1–15. DOI: http://dx.doi.org/10.1145/3173574.3173688

[16] Nigel Halpern, Deodat Mwesiumo, Thomas Budd, Pere Suau-Sanchez, and Svein Bråthen. 2021. Segmentation of passenger preferences for using digital technologies at airports in Norway. *Journal of Air Transport Management* 91 (2021), 102005. DOI: http://dx.doi.org/https://doi.org/10.1016/j.jairtraman.2020.102005

[17] Foad Hamidi, Morgan Klaus Scheuerman, and Stacy Branham. 2018. Gender Recognition or Gender Reductionism?: The Social Implications of Embedded Gender Recognition Systems. In *CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. DOI: http://dx.doi.org/10.1145/3173574.3173582

[18] Rakibul Hasan. 2020. Reducing Privacy Risks in the Context of Sharing Photos Online. (2020). DOI: http://dx.doi.org/10.1145/3334480.3375040

[19] Tadayoshi Kohno Ivan Evtimov, Pascal Sturmfels. 2020. FoggySight: A Scheme for Facial Lookup Privacy. (2020). DOI:http://dx.doi.org/arXiv:2012.08588

[20] A. Juels, D. Molnar, and D. Wagner. 2005. Security and Privacy Issues in E-passports. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*. 74–88. DOI: http://dx.doi.org/10.1109/SECURECOMM.2005.59

[21] T. A. M. Kevenaar, G. J. Schrijen, M. van der Veen, A. H. M. Akkermans, and F. Zuo. 2005. Face recognition with renewable and privacy preserving binary templates. In *Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05)*. 21–26. DOI: http://dx.doi.org/10.1109/AUTOID.2005.24

[22] Ruggero Donida Labati, Angelo Genovese, Enrique Muñoz, Vincenzo Piuri, Fabio Scotti, and Gianluca Sforza. 2016. Biometric Recognition in Automated Border Control: A Survey. *ACM Comput. Surv.* 49, 2, Article 24 (June 2016), 39 pages. DOI: http://dx.doi.org/10.1145/2933241

[23] Ruggero Donida Labati, Angelo Genovese, Enrique Muñoz, Vincenzo Piuri, Fabio Scotti, and Gianluca Sforza. 2015. Automated Border Control Systems: Biometric Challenges and Research Trends. In *Information Systems Security*, Sushil Jajoda and Chandan Mazumdar (Eds.). Springer International Publishing, Cham, 11–20.

[24] Melisa Locker. 2020. Report: 20 major airports may get face recognition for international travelers by 2021. (2020). https://www.fastcompany.com/90318183/20-major-airports-may-mandate-face-recognition-for\-international-travelers-by-2021

[25] Afra Mashhadi. 2020. A Privacy-Preserving Framework for Collecting Demographic Information. (2020). DOI: http://dx.doi.org/10.1145/3334480.3382800

[26] Pieter Simoens Mattijs Baert, Sam Leroux. 2020. Intelligent Frame Selection as a Privacy-Friendlier Alternative to Face Recognition. (2020). DOI: http://dx.doi.org/arXiv:2101.07529

[27] John Mears. 2017. Lift-off: can biometrics bring secure and streamlined air travel? *Biometric Technology Today* 2017, 2 (2017), 10–11. DOI:http://dx.doi.org/https://doi.org/10.1016/S0969-4765(17)30035-8

[28] Nasir Memon. 2017. How Biometric Authentication Poses New Challenges to Our Security and Privacy [In the Spotlight]. *IEEE Signal Processing Magazine* (2017). DOI:http://dx.doi.org/10.1109/MSP.2017.2697179

[29] Cristian Morosan. 2016. An empirical examination of U.S. travelers' intentions to use biometric e-gates in airports. *Journal of Air Transport Management* 55 (2016), 120–128. DOI:http://dx.doi.org/https://doi.org/10.1016/j.jairtraman.2016.05.005

[30] Cristian Morosan. 2018. Information Disclosure to Biometric E-gates: The Roles of Perceived Security, Benefits, and Emotions. *Journal of Travel Research* 57, 5 (2018), 644–657. DOI: http://dx.doi.org/10.1177/0047287517711256

[31] Nathane Ana Rosa Negri, Giovanna Miceli Ronzani Borille, and Viviane Adriano Falcão. 2019. Acceptance of biometric technology in airport check-in. *Journal of Air Transport Management* 81 (2019), 101720. DOI: http://dx.doi.org/https://doi.org/10.1016/j.jairtraman.2019.101720

[32] Elaine M. Newton. 2005. Preserving Privacy by De-Identifying Face Images. *IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING* (2005). https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1377174

[33] US Homeland Security. 2008. "The Fair Information Practice Principles". (2008). https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-prac

[34] Evan Selinger and Brenda Leong. 2021. *The Ethics of Facial Recognition Technology*. DOI: http://dx.doi.org/10.2139/ssrn.3762185

[35] Aaron Smith. 2019. More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly. (2019). https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-\trust-law-enforcement-to-use-facial-recognition-\responsibly/

[36] Erkin Z; Franz M; Toft T. 2009. Privacy enhancing techologies. (2009).

[37] Pagona Tsormpatzoudi, Diana Dimitrova, Jessica Schroers, and Els Kindt. 2015. Privacy by Design – The Case of Automated Border Control. In *Privacy and Identity Management for the Future Internet in the Age of Globalisation*, Jan Camenisch, Simone Fischer-Hübner, and Marit Hansen (Eds.). Springer International Publishing, Cham, 139–152.

[38] Hoo Keat Wong. 2020. The Own-Race Bias for Face Recognition in a Multiracial Society. *Front Psychol* 11, 208 (2020). DOI:http://dx.doi.org/https://doi.org/10.3389/fpsyg.2020.00208

[39] Daoxing Li Yuancheng Li, Yimeng Wang. 2019. Privacy-preserving lightweight face recognition. *Neurocomputing* (2019). DOI: http://dx.doi.org/10.1016/j.neucom.2019.07.039

APPENDIX

Content of Survey

Screening

1. How old are you? You must be at least 18 years old to complete this survey.
   - ○ Under 18
   - ○ 18-24
   - ○ 25-34
   - ○ 35-44
   - ○ 45-54
   - ○ 55-64
   - ○ 65-74
   - ○ 75-84
   - ○ 85 or older

   Some airports now use facial recognition and other biometrics to verify travelers' identities. Below are two examples of systems that perform this automatic verification.
2. At United States airports, has your identity ever been verified using facial recognition?
   - ○ Yes
   - ○ No
   - ○ Unsure
   - ○ I have used facial recognition at an airport, but I'm not sure if it was within the United States.
3. At United States airports, have you ever opted out of using facial recognition to verify your identity?
   - ○ Yes
   - ○ No

Usage information

1. In which scenario(s) was facial recognition used to verify you? Select all that apply.
   - □ At check-in
   - □ At a security checkpoint
   - □ When boarding
   - □ At border control (leaving the United States)
   - □ At border control (entering the United States)
2. At which location(s) was facial recognition used to verify you? Select all that apply.
   - □ Boston Logan International Airport (Boston, MA)
   - □ Charlotte Douglas International Airport (Charlotte, NC)
   - □ Chicago O'Hare International Airport (Chicago, IL)
   - □ Dallas/Fort Worth International Airport (Fort Worth, TX)
   - □ Detroit Metropolitan Wayne County Airport (Detroit, MI)
   - □ Dulles International Airport (Sterling, VA)
   - □ Fort Lauderdale-Hollywood International Airport (Fort Lauderdale, FL)
   - □ George Bush Intercontinental Airport (Houston, TX)
   - □ Hartsfield-Jackson Atlanta International Airport (Atlanta, GA)
   - □ JFK International Airport (Queens, NY)
   - □ Los Angeles International Airport (Los Angeles, CA)
   - □ McCarran International Airport (Las Vegas, NV)
   - □ Miami International Airport (Miami, FL)
   - □ Minneapolis-Saint Paul International Airport (Minneapolis, MN)
   - □ Newark International Airport (Newark, NJ)
   - □ Norman Y. Mineta San Jose International Airport (San Jose, CA)
   - □ Orlando International Airport (Orlando, FL)
   - □ Ronald Reagan Washington National Airport (Arlington, VA)
   - □ Salt Lake City International Airport (Salt Lake City, UT)
   - □ San Diego International Airport (San Diego, CA)
   - □ San Fransisco International Airport (San Mateo, CA)
   - □ Seattle-Tacoma International Airport (Seattle, WA)
   - □ Tampa International Airport (Tampa, FL)
   - □ William P. Hobby Airport (Houston, TX)
   - □ Other (US only - please specify)
   - □ Unsure
3. How far in advance were you made aware that facial recognition systems would be used to verify you at the airport?
   - ○ During a pre-registration process
   - ○ When purchasing tickets/planning the trip
   - ○ At check-in
   - ○ Just before using the facial recognition system
   - ○ I don't remember
4. To your knowledge, was the use of facial recognition required at any point?
   - ○ Yes
   - ○ No
5. Please select your level of agreement with the following statements. (Options are the same for each statement.)
   - I care about the privacy of my personal information.

- Strongly agree
- Somewhat agree
- Neither agree nor disagree
- Somewhat disagree
- Strongly disagree

- I want to know in advance if facial recognition will be used to identify me.
- The use of facial recognition makes air travel more efficient.
- The use of facial recognition at airports means every traveler is treated fairly.
- The use of facial recognition at airports makes it harder for unauthorized travelers to proceed.
- Images of my face are sensitive information.
- Facial recognition algorithms are sometimes unfair towards certain people.
- If I use facial recognition at the airport, it is because I actively signed up for it.
- Before traveling, I read the terms and conditions of the airline I will use.
- When I use facial recognition at the airport, I trust that my data is stored securely.
- I feel comfortable giving airports access to my facial recognition data.
- Facial recognition algorithms can identify travelers more accurately than a human can.
- I feel comfortable giving US border authorities access to my facial recognition data.
- I can choose not to use facial recognition during air travel.
- I know exactly how my facial recognition data will be used by airports or border authorities.

6. In future air travel, would you prefer to use facial recognition, some other biometric, or manual methods to verify your identity?
   - Facial recognition
   - Other biometrics (e.g., fingerprints)
   - Manual verification (e.g., ID inspection by a border agent)
7. Please explain your answer to the previous question.

Demographics

1. Before 2020, about how often did you travel on an airplane?
   - Very rarely
   - Once every few years
   - 1-2 times a year
   - 3-8 times a year
   - Once a month
   - More than once a month
   - I have never been on an airplane.
2. In which year did you most recently travel on an airplane?
   - 2021
   - 2020
   - 2019
   - 2018
   - 2017 or earlier
3. Before 2020, about how often did you travel across the United States border?
   - Very rarely
   - Once every few years
   - Once a year
   - Multiple times a year
   - I have never crossed the United States border.
4. What is your gender?
   - Male
   - Female
   - Non-binary / third gender
   - Prefer not to say
5. What is your ethnicity? Select all that apply.
   - ☐ White
   - ☐ Black or African American
   - ☐ American Indian or Alaska Native
   - ☐ Asian
   - ☐ Native Hawaiian or Pacific Islander
   - ☐ Latinx
   - ☐ Other
6. What is your highest education level?
   - Less than high school
   - High school graduate
   - Some college
   - 2 year degree
   - 4 year degree
   - Professional degree
   - Doctorate