Report 2019-01 of the DHS Data Privacy and Integrity Advisory Committee (DPIAC): Privacy Recommendations in Connection with the Use of Facial Recognition Technology

As approved in Public Session on February 26, 2019

Summary of Request and Context

The Department of Homeland Security's (DHS's) missions include preventing terrorism and enhancing security, managing our borders, administering immigration laws, securing cyberspace, and ensuring disaster resilience. Certain DHS components collect and use sensitive personally identifiable information (PII) for operational use in its various missions.

One of these components, U.S. Customs and Border Protection (CBP), is charged with keeping terrorists and their weapons out of the U.S. while facilitating lawful international travel and trade. The men and women of CBP are responsible for enforcing hundreds of U.S. laws and regulations. On a typical day, CBP welcomes nearly one million visitors, screens more than 67,000 cargo containers, arrests more than 1,100 individuals, and seizes nearly 6 tons of illicit drugs. Annually, CBP facilitates an average of more than $3 trillion in legitimate trade while enforcing U.S. trade laws.[1]

CBP continues to implement advanced technologies to assist in its mission – including the use of biometric technology, screening, and facial recognition systems to identify and confirm the identities of persons traveling to and from the U.S. through its biometric entry-exit system for international flights at airports throughout the U.S. CBP has partnered with commercial air carriers and airport authorities that capture facial images of travelers as part of their business processes, and send those images to CBP for use in the Traveler Verification Service (TVS). CBP matches the images against previously-captured photos by using a cloud environment to verify the identity of the traveler across the international border.

The ultimate goals of CBP by strengthening the biometric entry-exit program are to make air travel and/or land travel: (1) more secure, by providing increased certainty as to the identity of airline travelers at multiple points in the travel process, and (2) more predictable, by establishing a clear, easily-understood boarding process. CBP also seeks to build additional integrity into the immigration system, by better identifying which foreign nationals are violating the terms of their admission into the United States, and by providing the capability for immediate action when that occurs.

In addition, the DPIAC acknowledges that there are unique operational differences depending on the location of screening, physical environment, external elements (e.g., nature), and threat risks that may impact the recommendation made here. Generally, this report focuses on the use of facial scanning biometrics upon exit from the U.S., but many of its thematic recommendations may apply to biometric screening at other locations. It is important to note this Report only addresses the requests of the DHS Privacy Office from its September 11, 2017 Tasking and is meant to be responsive to the specific questions asked in this Tasking and not made more widely applicable to the overall topic of biometric facial recognition outside the programs reviewed. Further it is critical for the success of the Biometric Exit Program and/or other biometric programs that data intended to be used only for screening purposes is not further transferred, shared, or used for other purposes, including without limitation private-sector purposes (e.g. marketing) or other government purposes (e.g. law enforcement or intelligence purposes).

[1] CBP mission and facts at https://www.cbp.gov/about.

I. Tasking

On September 11, 2017, the DHS Chief Privacy Officer requested that the DPIAC provide guidance on best practices for the use of biometrics, specifically facial recognition technology, for identification purposes. The tasking asked the following:

- How can CBP provide adequate and meaningful notice in both airports and land border environments to individuals regarding the collection of biometrics from new populations and at exit, where most travelers have not typically encountered CBP in the past?
- Are there standards or guidance CBP should take into consideration when determining how long a photo is useful and reliable for facial recognition purposes? How might that range vary depending on the age of the subject (for example, how does the reliability of a match based on a photo of a 15-year old who is now 24 compare to an old photo of an older adult)?
- Facial matching algorithms have often proven less accurate with certain demographic groups. What are business standard measurements for ensuring facial recognition accuracy across all demographics? Please provide recommendations for matching against a small fixed gallery (one-to-few) as well as general large gallery (one-to-many).
- It is extremely resource consuming for trained CBP Officers to operate the cameras at the boarding gates; how can CBP best leverage private industry to facilitate this collection? What sort of data protections should the government pursue with private industry?

This report represents the results of that review and addresses a number of recommendations related to the DHS Privacy Office's request.

II. Introduction and Fact Finding

A. Introduction

Identification is a significant portion of CBP's responsibility and legal mandate under numerous laws and Executive Orders.[2] Identification is a critical pre-requisite to authorizing access and assessing potential threats.

Facial recognition biometrics uses an individual's face to identify or verify the identity of the individual. Facial recognition systems can be used to identify people in photos, videos, or in real-time. The technology works by first capturing an image of a person's face. The image is cropped and converted into a mathematical representation called a "face template" or "template." The face template is designed only to include certain details that can be used to distinguish one face from another, including the distance between the eyes, the shape of the chin and the length of the nose. Algorithms in facial recognition systems will compare the template with other templates on file and calculate the similarity of two images being compared.

Some systems are designed to accept the match if the calculated level of similarity of the presented images is equal to or greater than a predetermined probability level and to reject it if it is less than the

[2] The 1996 Illegal Immigration Reform and Immigrant Responsibility Act authorized an automated system to record arrivals and departures of non-U.S. citizens at all air, sea, and land ports of entry. The 2002 Enhanced Border Security and Visa Entry Reform Act, the Intelligence Reform and Terrorism Prevention Act of 2004, and the Implementing Recommendations of the 9/11 Commission Act of 2007, all called for the creation of a nationwide biometric entry-exit system. The Consolidated Appropriations Act of 2016 authorized CBP to expend up to $1 billion in certain visa fee surcharges collected over the next ten years for biometric entry and exit implementation. Executive Order 13780, "Protecting the Nation from Foreign Terrorist Entry into the United States," required DHS to "expedite the completion and implementation of a biometric entry-exit tracking system for in-scope travelers to the United States."

probability level. Other systems are designed to calculate a probability match score between the unknown person and specific face templates stored in the database. Rather than accept or reject based on the match probability score, the system will offer several potential matches, ranked in order of likelihood of correct identification, instead of just returning a single result. In these systems, human intervention is necessary to down-select from the group.

As used in the current implementation, CBP uses a system that informs the traveler, CBP, and airline personnel that the person is either a match or not a match with an image they have on file, as opposed to any further probability analysis. As employed in the Biometric Exit Program, the steps of facial recognition identification are:

- The TVS uses CBP's biographic Advanced Passenger Information System (APIS) manifest data and existing photographs of all travelers boarding international flights to confirm the identity of the traveler, create an exit record, and biometrically confirm the exit of non-U.S. citizens. These images include photographs taken by CBP during the entry inspection, photographs from U.S. passports and U.S. visas, and photographs from other DHS encounters.
- Using the flight manifest, CBP builds a flight photo gallery for that specific flight.
- As boarding begins, each traveler approaches the departure gate to present a boarding pass and stands for a photo in front of a camera that is owned either by CBP or by a partner airline or airport authority. The camera securely transmits usable images to CBP's cloud-based TVS facial matching service. The TVS returns faces that best match the reference face, thus verifying the identities of individual travelers. If a match is found, the traveler is informed through visual and auditory cues, if a gate is present it opens, and the traveler proceeds to the aircraft. If the TVS cannot verify the identity of the traveler, the identity of the traveler is confirmed manually (i.e. the traditional way boarding is conducted) through their travel documents by gate personnel.
- If the photo taken at boarding is matched to a U.S. passport, the traveler having been confirmed as a U.S. citizen is automatically determined to be out of scope for biometric exit purposes and the photo is discarded after a short period of time.

B. Fact Finding

In order to understand how CBP can provide adequate and meaningful notice to individuals in airport and other border environments regarding the collection of individual biometrics from new populations and at exit, DPIAC members engaged in numerous meetings over the course of several months. It is important to highlight the nature and extent of these meetings as they were required to gain an understanding of the programs, controls, and challenges associated with implementation of facial recognition technology. In addition, the DPIAC believed that it would be in a position to provide more accurate and operationally sound guidance after reviewing the biometric exit program live. The review activities included:

- September 19, 2017 – Briefing on Biometric Travel Security Initiative (open to the public)
- May 9, 2018 – Briefing by Laura Moy (Deputy Director at the Center on Privacy & Technology, Georgetown Law) and Harrison Rudolph (Associate at the Center on Privacy & Technology at Georgetown Law) regarding privacy, security, operational, and legal concerns with the use of facial recognition technology from the 2017 Georgetown Law paper[3]
- May 11, 2017 – Meeting with CBP on the specific facial recognition technology being used, policy notices, awareness, and privacy impacts
- July 10, 2018 – In person, half-day review of a facial recognition pilot program at the Orlando International Airport (MCO) that included CBP operations at entry and exit, biometric exit flight operations at a British Airways boarding gate, and biometric scanning technology and operations.

[3] Georgetown Law Center on Privacy & Technology, *Not Ready for Takeoff: Face Scans at Airport Departure Gates*, December 21, 2017. See https://www.airportfacescans.com/.

Participating in this review were members of the DHS Privacy Office, CBP, DPIAC, as well as numerous personnel on the ground at MCO.

In addition, the DPIAC relied on prior Privacy Impact Assessments (PIAs) that are publicly available[4] on the DHS website for additional information and CBP's website on biometric use, specifically:

- PIA for the Departure Information Systems Test - DHS/CBP/PIA-030) (June 13, 2016)
- PIA for the Departure Verification System - DHS/CBP/PIA-030(a) (December 16, 2016)
- PIA for the Traveler Verification Service (TVS) - DHS/CBP/PIA-030(b) (May 15, 2017)
- PIA for the Traveler Verification Service (TVS): Partner Process - DHS/CBP/PIA-030(c) (June 12, 2017)
- PIA for the Traveler Verification Service (TVS): CBP-TSA Technical Demonstration - DHS/CBP/PIA-030(d) (September 25, 2017)
- PIA for the Traveler Verification Service (TVS): CBP-TSA Technical Demonstration Phase II - DHS/CBP/PIA-030(d) (August 14, 2018)
- PIA for the Traveler Verification Service: DHS/CBP/PIA-056 (November 14, 2018)[5]

C. Review Areas

The DPIAC considered the question posed in this tasking by reviewing the following four aspects of facial recognition and biometric usage: (1) Transparency, (2) Data Minimization, (3) Data Quality & Integrity, and (4) Accountability & Auditing. Each is discussed below along with recommendations for further consideration.

III. Transparency

The DPIAC reviewed notices used in connection with the collection of biometrics in various meetings with CBP and in person at MCO Airport. These notices were posted in the International Arrivals Area at MCO for biometric entry screening and at the departure gate for travelers exiting the U.S (biometric exit). The notices viewed in person were the same as or similar to notices contained in CBP briefing materials and on the CBP website. Members of the DPIAC who participated in person at MCO in July 2018 also heard information similar to that contained on these notices announced over the loudspeaker at the boarding gate prior to the flight. Based on these meetings and observations, we recommend the following substantive and procedural measures to achieve transparent and timely notice to international travelers, including U.S. citizens:

A. Substantive Notice

The content of the notices must be meaningful to the intended recipients, especially new populations. This requires that they be easy to read and understand. We recommend that notices meet established readability standards, such as the Flesch Readability Ease Score or the Flesch-Kincaid Grade Level Score.

The presentation of written notices should be in a font and color that is easily seen and read. Notices should be available both in English and appropriate other languages, such as those used on Visa forms, signs in the Embassy or Visa office in the country of flight origin, or reflecting the nationality of the relevant airline.

---

[4] See https://www.dhs.gov/publication/departure-information-systems-test.

[5] The November 2018 PIA from DHS regarding the TVS was received after the DPIAC had reviewed the TVS programs and provided oral commentary to DHS. As such, many of the observations contained in this Report are in fact represented and included in the latest PIA. The simplification and consolidation of all previous PIAs on TVS by CBP into the November 2018 PIA is more comprehensive and serves as an important reference for privacy and security recommendations and implemented controls.

The notices should briefly explain the reasons for the information capture, the security associated with the process, storage/deletion of the data, any other uses of the data, choices or opt-outs of data collection, consequences of exercising an opt-out, and redress rights in the event of a mismatch.

In addition to testing notices for readability, as discussed above, the DPIAC suggests that additional pilots and longitudinal measurement of notice effectiveness on various populations of international travelers may yield further insights and opportunities for streamlining.

B. Procedural Notice

Several members of the DPIAC viewed the notice process for air travel from the point of view of a passenger arriving in or leaving the U.S., both to (i) eliminate surprise and delays in the process, and (ii) allow passengers time to consider thoughtfully the substance of the notices, understand what their consent means, and determine if they would like to consent.

> *Before Boarding:* Written notices should be provided as part of visa application disclosures and notices, and signage should be posted at kiosks or boards in visa collection and processing offices as appropriate. Airline websites describing the documentation needed for a flight to the U.S. should include the relevant notices, allowing passengers to read them during the planning, ticketing, and check-in processes for their flights.
>
> *On-Board Flights to the U.S.:* Notices should be provided by in-flight crew as part of the entry documentation distributed prior to landing. Written notices may be disseminated as part of entry and customs forms, or included in in-flight magazines, for example. Crews should draw attention to the information in the language(s) used for flight announcements.
>
> *Upon Arrival in the U.S.:* Notices should be provided via posters, signs, and tear-sheets available to passengers. Prominence should be given to the rights of individuals, how they can exercise their rights, and the impacts of exercising those rights (such as increased screening time and longer lines). If there is a hyper-link or website noted, these notices should be given in an area where passengers are allowed to use mobile devices to view the hyper-link or website information in advance of making the decision to enter the U.S. and/or electronic displays should display the linked materials.

These guidelines may be easily adapted to cruise lines because many of the same passenger procedures are used: websites, check-ins, on-board announcements, distribution of entry documentation, and dedicated customs and immigration sites.

Land and other border environments are more complex. Bus and train lines have notices on websites, paper documentation, and departure stations, which may be analogous to air travel. Private car transportation at borders have fewer opportunities for meaningful notice before the border crossing. Notices may be placed at nearby road services plazas or on billboards, but they will necessarily be less effective in reaching all affected travelers. Internet and paper map service providers may choose to link to the relevant notices where they show border crossings.

C. Contact Information

CBP should also ensure that notices, signage, websites or other means of communication include a "Contact Us" section should the individual wish to make an access request, inquiry, or complaint.

D. Summary of Recommendations – Transparency

CBP should seek to ensure notice readability and effectiveness by catering to different learning levels, languages, and nationalities. CBP can better understand how to effectively manage this through testing and evaluation. CBP also should ensure that travelers have sufficient time and the opportunity to review the relevant privacy notices and/or hyperlinks referenced in the notices, especially in connection with varied forms of transportation and border crossings.

IV. Effectiveness & Data Minimization

How long an image is useful in comparing the person before a CBP agent to prior images is a key question and can increase screening effectiveness. The DPIAC interprets the question "how long a photo is useful and reliable for facial recognition purposes" to mean: "How many years between the age of the person when the initial sample image was created and the age of the person at the time the comparison sample image was taken constitutes a 'usable' and 'reliable' period of time to reliably deliver a match of images of the same person."

> *Put simply*: How long does it take for the human face to become unrecognizable to facial recognition systems?
>
> *Put technically*: What is the ratio of successful matches of a "probe (query)" image and its "enrollment (gallery) image"[6] to the age (changes) of the person (as measured by the template match success/failure rates over time)?[7]

There are additional factors which affect the accuracy of facial recognition systems, but these questions are scientific and technical research questions and the DPIAC recommends that they be supported and addressed by DHS's Science & Technology Directorate (DHS S&T). [8]

A. Time Period and Effectiveness

DPIAC conducted initial research and identified at least one industry standard of approximately 8.5 years for reliable facial recognition based on the changes of a person's body (face) over time.

- A recent study presented at the Computer Vision and Pattern Recognition Workshops (CVPRW), 2017 IEEE Conference entitled, "*Face Recognition Performance under Aging*",[9] looked at the performance of two state-of-the-art commercial facial recognition systems on two large-scale longitudinal datasets.
- Based on the results of their statistical model, the commercial systems verified 99% of the subjects at a false accept rate of 0.01% for up to 10.5 and 8.5 years of elapsed time. Beyond this time period there is a significant loss in facial recognition accuracy. The authors claim the study extends and confirms the findings of earlier longitudinal studies on facial recognition.[10]

This research seems to set the acceptable period of human aging to a maximum of 10.5 years and a reliable period of 8.5 years. The DPIAC recommends that CBP engage with other experts in Science and Technology (DHS S&T) and the National Institute of Standards and Technology (NIST) to perform reliability testing to further hone in on accuracy metrics and an appropriate number of years of reliability for various age bands (i.e. more facial changes for those under 14 years of age than other populations).

---

[6] *Abstract*, "*Face Recognition Performance under Aging*", http://ieeexplore.ieee.org/document/8014816, visited July 13, 2018.

[7] Template data comparison and accuracy may be affected by multiple factors – all but one are outside the scope of this report. DPIAC recommends the DHS Privacy Office collaborate with the DHS Science & Technology Directorate to identify and address those additional factors. The privacy concern is that DHS collects the least amount of personal information from affected individuals and use that information only as necessary and then destroy it. If DHS discovers that, for whatever reason, it possesses biometric data that is useless, DPIAC recommends DHS destroy that data and only retain data proven to be necessary and useful.

[8] "[A]ccuracies of face recognition systems are adversely affected by factors including facial pose, illumination, expression and aging, collectively known as PIE-A." *Introduction*, "*Face Recognition Performance under Aging*", http://ieeexplore.ieee.org/document/8014816, visited July 13, 2018.

[9] http://ieeexplore.ieee.org/document/8014816, visited July 13, 2018.

[10] *Abstract*, "*Face Recognition Performance under Aging*", http://ieeexplore.ieee.org/document/8014816, visited July 13, 2018.

CBP may also want to correlate this optimal number, but suggests that it match this time threshold to the expiration time for travel credentials and accuracy criteria when examining images older than 10.5 years.

B. Reliability in Biometric Exit

For each applicable flight, CBP prepares a gallery of images for those individuals expected to enter or exit the next day and as the manifest is updated the day of travel. The DPIAC heard from members of CBP how they use the matching analysis to review the overall reliability of the biometric exit program. It is important for CBP to provide additional transparency into reliability, deviations, and other statistical data to measure both real-world and test-based system applications. By providing this additional information, CBP will better inform the public and it may also encourage additional research and testing into rejection rates.

C. Data Minimization

DHS formalized its principles to align its practices to the Fair Information Practice Principles (FIPPs) in 2008.[11] DPIAC acknowledges that CBP has implemented a mechanism to retain the images of U.S. Citizens electing to use biometric exit for no more than 14 days and these efforts to retain PII for only as long as necessary are valuable methods to strengthen privacy.

D. Summary of Recommendations – Data Minimization

1. DHS Science & Technology (S&T) Collaboration - True technical accuracy and reasonable thresholds of acceptability are scientific and technical research issues. CBP and DHS S&T can also partner with NIST to draw from additional research of existing standards and practices as well as the opportunity to create new industry standards to address new or nuanced challenges in the facial recognition research & practice space.
2. Image Use Over Time - Based on DPIAC's initial research, DPIAC recommends DHS research the usefulness of images with other partners from DHS S&T, NIST, and the larger community of researchers. Based on DPIAC's review of the literature, the lowest failure rates were seen with when comparing images of the individual from within 8.5 – 10.5 years of the date the original photo.[12]
3. Data Minimization - CBP should only retain and use personal information that is necessary to delivery its legally mandated obligations.[13] Efforts should be taken to minimize the capture of images of individuals whose age is outside of prescribed ranges.

V. Data Quality & Integrity

A. The DHS Biometric Exit/Entry System

Accuracy is a major concern with the use of facial recognition technology. When accuracy is low, a person can be incorrectly identified as another person in the data base (false acceptance). If this occurs in the biometric exit program, a person will be able to board the plane using a false identity.

---

[11] "Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security." https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles, visited July 13, 2018.

[12] Based on portion of the article DPIAC identified earlier in this document.

[13] "Data Minimization: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s)." https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf, visited July 13, 2018.

Low accuracy can also fail to confirm a person's identity by not matching a current facial scan with scans or images stored in the database (false rejection). However, in the present case when a person is rejected as a non-match, the person's identity will be confirmed by using their passport photograph.

B. Ensuring Accuracy

The accuracy of facial recognition systems has improved significantly in recent years.[14] A recent report from NIST (November 2018) concluded that "massive gains in accuracy have been achieved in the last five years (2013-2018) and these far exceed improvements made in the prior period (2010-2013)". In fact, the November 2018 NIST Report states that with good quality portrait photos, the most accurate algorithms have "error rates below 0.2%".[15]

However, various reports of inaccuracy tied to biometric screening (especially facial scanning) have been issued over the past few years. DHS should take the lead to work with technical partners and the broader research community to ensure accuracy standards, guidelines, and effectiveness/error percentages are included in all uses of facial recognition deployments and that these are updated on a yearly basis as needed. As DHS and its partners work with various vendors of biometric technology, DHS should contractually require periodic reports on the accuracy, effectiveness, and error reporting of similar factors/demographic factors with an eye on continual improvement. These reports should be granular and targeted at precise demographic and other similar characteristics that allows for the cross-comparison of technologies, vendors, and implementations. These recommendations are important to mitigate the following factors that may lessen accuracy and data quality for facial recognition systems:

- The type and size of the database (used for matching purposes);
- Poor or uncontrolled environment where the image is captured (e.g., angle of view or illumination, single person or real-time);
- Low-quality image or viewing resolution;
- Facial expression;
- Aging (age-related changes in the face); and
- Demographics (racial and ethnic factors and gender).

<u>Type and Size of the Database</u>

The accuracy of facial recognition technology often suffers in one-to-many facial recognition systems where the system is matching faces against a large database of photos instead of just one photo. On the other hand, matching a face template of a person against a smaller database of templates in the system (one-to-few) will have a higher level of accuracy.

The Biometric Exit Program at air and sea points of entry compares the face template taken at the departure gate with the template created from the traveler's passport photo - a one-to-few database comparison that commonly offers a higher accuracy rate than comparing a captured face template against a large database of templates.

<u>Poor or uncontrolled environment</u>

The environment where the face scan occurs has the potential to impact the data integrity. If a room is dark it will be more difficult to match the scan to the image in the database. If the person is moving or the angle of the scan is poor, the integrity of the scan can be harmed.

[14] Paying with Your Face: Face-detecting systems in China now authorize payments, provide access to facilities, and track down criminals. Will other countries follow?, Will Knight, MIT Technology Review, March April 2017.
[15] NISTIR 8238: Ongoing Face Recognition Vendor Test (FRVT) Part:2 Identification (November 2018) at https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf.

However, CBP requires system partners to provide state-of-the-art face matching systems in the Biometric Entry/Exit program. The cameras used in the program have an accuracy goal of 96% true acceptance rate (TAR).[16] The cameras are required to: (i) capture multiple images; (ii) draw the traveler's attention to the camera and hold it during the image taking process; (iv) include a time-out function to ensure that the best captured image of the traveler is used if an image does not meet the desired quality threshold; (iv) and provide proper lighting.[17]

The facial recognition systems used in the biometric exit program at MCO were located in controlled environments with sufficient lighting and provide clear instructions to the subject on how to pose to provide a frontal scan. Proper positioning of the subject and high level of illumination will result in a more accurate scan and make it easier to match it to the image of the person in the database.

Low-quality image or viewing resolution

The cameras used in the Biometric Exit/Entrance program vary at each location, but the DPIAC recommends ensuring they are of sufficient resolution at all locations to take a picture at the recommended resolution. The system provides a green indicator when there is a match and a red indicator when the identity of the person cannot be verified. If this occurs, the CPB or airline personnel review the person's passport picture to confirm the identity of the person who is boarding and not the image captured at the gate.

Expression

Facial expression is another factor that can alter the data integrity of facial recognition technology. In recent years passport applicants have been instructed to have a neutral expression and fully opened eyes in passport photos. It is likely that the face templates used in the TVS system will have a neutral expression. Comparing neutral expressions will enhance accuracy in the matching process.

Age

In a study on what effects facial aging has on the performance of automatic facial recognition systems using mugshot databases, the research team found that 99% of the face images can still be recognized up to six years later.[18] DPIAC recommended CBP work with DHS S&T and NIST to examine impacts on the length of time photos are useful before degrading the accuracy of a match.

[16] Privacy Impact Assessment Update for the Traveler Verification Service (TVS): Partner Process DHS/CBP/PIA-030(c) June 12, 2017 pp. 13-14, Hereinafter, "2017 PIA"). According to the 2017 PIA, the DHS Science and Technology Directorate (S&T) is generating a report identifying how each algorithm performed as a true positive rate, false positive rate, false match rate, and false non-match rate.
[17] Id.
[18] Longitudinal Study of Automatic Face Recognition, Anil K. Jain, Lacey Best-Rowden, EEE Transactions on Pattern Analysis and Machine Intelligence Journal, Volume 40, Issue 1, January 1, 2018.

Demographics

Facial matching algorithms have been shown to be less accurate with certain demographic groups.[19] A 2012 study co-authored by the FBI showed that accuracy rates for African Americans were lower than for other demographics.[20] Face recognition software has been found to misidentify other ethnic minorities, young people, and women at higher rates.[21]

Recently, facial recognition vendors have announced significant improvements in their system's ability to recognize gender across skin tones.[22] With the improvements, the vendor said it was able to reduce the error rates for men and women with darker skin by up to 20 times. To reach these results the software team made three major changes. They expanded and revised training and benchmark datasets, launched new data collection efforts to further improve the training data by focusing specifically on skin tone, gender and age, and improved the classifier to produce higher precision results.

C. Summary of Recommendations – Data Quality & Integrity

1. In addition to the reporting requirements from vendors and partners described above, DHS should provide additional auditing around these requirements and the performance of all biometric systems. DHS should aggregate these reports into one report that can be released to the public on at least an annual basis. This report should include granular data on the efficacy of biometric systems especially as it relates to persons of different demographics and similar characteristics.
2. DHS should provide additional transparency around the accuracy of the biometric systems being used and specifically metrics for the types of populations that have been noted above.
3. DHS should ensure that DHS Components, other government entities, partners, and vendors protect the information they are capturing. Establish data use and retention guidelines that prohibit, as appropriate, use of data beyond the purposes for which it is collected.
4. CPB should train partner airlines on how to use the systems, protect information being collected and increase transparency for travelers.
5. DHS should work with NIST, DHS S&T, and other academic or research organizations to ensure the most stringent algorithmic and technical standards are upheld to minimize disparity of accuracy in identification related to race, color, ethnicity, age, sex, and other similar factors.

VI. Accountability & Auditing

Within the parameters of the Biometric Exit Program, CBP partners with the airlines and airline personnel. In some instances, CBP may be present or operate equipment for biometric exit screening, but in most cases the airline is the partner actually clearing the passenger. The DPIAC witnessed such a collaborative partnership at MCO between CBP and British Airways gate personnel.

When biometric screening equipment is operated in part or entirely by partners it is important to ensure transparency in the process, strong contractual guidelines, auditing, and rigor in the process of ensuring the FIPPs are adhered to. Below are some key considerations CBP should ensure are engrained into the Biometric Exit Program.

---

[19] Are Face Recognition Systems Accurate? Depends on Your Race, Mike Orcutt, MIT Technology Review, July 6, 2016.

[20] Face Recognition Performance: Role of Demographic Information, Brendan F. Klare*, Member, IEEE*, Mark J. Burge*, Senior Member, IEEE*, Joshua C. Klontz, Richard W. Vorder Bruegge*, Member, IEEE*, and Anil K. Jain*, Fellow, IEEE,* IEEE Transactions on Information Forensics and Security, VOL. 7, NO. 6, December 2012, available at https://assets.documentcloud.org/documents/2850196/Face-Recognition-Performance-Role-of-Demographic.pdf.

[21] Microsoft improves facial recognition technology to perform well across all skin tones, genders, Microsoft AI Blog June 26, 2018, available at https://blogs.microsoft.com/ai/gender-skin-tone-facial-recognition-improvement/

[22] *Id.*

Facial Biometric Collection:

- Consent regarding collection along with opt-in/opt-out options
- Transparency regarding the specific facial biometric collected
- Accountability and auditability regarding technology efficacy for facial recognition

Facial Biometric Analysis:

- Consent for limited use specific to identification
- Transparency regarding use specific to identification
- Provisions for no further onward transfer to other third parties or downstream use

Facial Biometric Protection:

- Accountability and auditability regarding technology efficacy of facial recognition
- Facial Biometric Data Protection
    - Transparency for information sharing (e.g. with whom) and storage (e.g. where)
    - Accountability and auditability regarding personnel and network access to sensitive facial biometric data as well as technology efficacy for security and privacy

A. Accountability and Auditing of Facial Biometric Collection and Analysis

Accountability and Auditing of facial biometrics must provide a means to evaluate collection methods that are aligned with and sensitive to the situation contexts. CBP must take steps with vendors to ensure reasonable facial biometric collections and analysis to include the following:

(1) Pre-engagement due diligence (e.g. Can the vendor support targeted collection benchmarks, collection transparency, and adherence to opt-in/opt-out standards?);
(2) Contract provisions (e.g. What core provisions are necessary for facial biometric collection to ensure technology efficacy and policy adherence, data analysis, assurance of limited use,); and
(3) Ongoing monitoring/compliance review (e.g. What steps should CBP take to ensure compliance to efficacy benchmarks for facial biometric collection technology and operational effectiveness in different situation contexts?).

B. Facial Biometric Data Protection

The protection of collected facial images along with associated PII is paramount. CBP must protect facial biometric data at collection and analysis while data is in use, in transit, and at rest (storage). Facial biometrics along with the associated personally identifiable information is at risk and in need of protection at enrollment, during analysis/use, in transit and at rest. These protections must recognize the risks posed by external threats as well as internal threats, both malicious insider threats and non-malicious due to negligence.

CBP must take steps with any vendor to ensure reasonable data protection to include but not limited to:

(1) Pre-engagement due diligence (e.g. Can the vendor support reasonable data protection practices?);
(2) Contract provisions (e.g. What core provisions are necessary re: data use, security, and compliance auditing?); and
(3) Ongoing monitoring/compliance review (e.g. What steps should CBP take to ensure compliance – for example, data use audits, log reviews, etc?).

The largest partner CBP will have in the Biometric Exit Program is the airlines and airline personnel. Based on our current understanding of the program, the airlines will not be receiving facial recognition data or results in this partnership. This is a preferred method to enable faster screening, higher rates of identity verification, offer a collaborative partnership with the airlines and the entities responsible for

airport operations, and balance the privacy and security interests of travelers. It will be critical for the success of the Biometric Exit Program and/or other biometric programs that data intended to be used only for screening purposes is not further transferred, shared, or used for other purposes, including without limitation private-sector purposes (e.g. marketing) or other government purposes (e.g. law enforcement or intelligence purposes). The DPIAC recommends contractual provisions reflecting these observations be implemented with any partners, especially the airlines and technology providers.

C. Leveraging Private Partnerships

The DPIAC notes that DHS S&T recently conducted a 2018 Biometric Technology Rally designed to provide a repeatable test methodology with which to measure the state of the biometric industry in regard to high-throughput systems .[23] This DHS 2018 Biometric Technology Rally was designed to measure the efficiency (throughput), effectiveness (capture capability, matching capability), and user satisfaction metrics of biometric systems that take under ten seconds to use on average.[24]

Allowing for the rapid deployment, testing, and socialization of facial scanning and other biometrics in a competitive but informative environment is an extremely valuable way to bring various DHS Components together and other vendors/stakeholders.

D. Summary of Recommendations – Accountability & Auditing

The DPIAC recommends that CBP:

1. Continue to work with other DHS Components and Industry Stakeholders to rapidly explore new technologies in a privacy and security forward manner.
2. Ensure through contractual provisions that data, images, and other information obtained through the screening of travelers is used for those limited purposes, done in a transparent manner, and subject to onward use restrictions.
3. Ensure through audits that technology use limitations are enforced as well as other contractual provisions.

VII. Conclusion

The Committee believes that the use of facial scanning biometrics to screen travelers both entering and leaving the U.S. is a technology that enhances the overall security of the U.S., speeds up screening processes, and may identify security risks. The DPIAC believes that the introduction of biometric screening technology should continue to be open and transparent, focus on mitigating privacy concerns of onward/third party use for other purposes, be operationally sound from an efficacy and screening perspective, and ensure the data security of all travelers.

[23] http://mdtf.org/rally/rally/RallyResults.html
[24] *Id.*

Appendix A – Summary of Recommendations

Recommendations – Transparency

- Ensure notice readability and effectiveness by different learning levels, languages, and nationalities through testing and evaluation.
- Ensure travelers have enough time and the opportunity to review privacy notices and/or any additionally mentioned hyperlinks referenced in the notices, especially for varied forms of transportation and border crossing.

Recommendations – Data Minimization

- Partner ***w***ith both DHS Science & Technology (S&T) and NIST to draw from additional research of existing standards and practices regarding biometric facial recognition.
- Based on DPIAC's review of the literature, the average usefulness of an original image is approximately 8.5-10.5 years from the date it was taken. DPIAC recommends DHS research the usefulness of images with other partners from DHS S&T, NIST, and the larger community of researchers.
- CBP should only retain and use personal information that is necessary to delivery its legally mandated obligations.

Recommendations – Data Quality & Integrity

- In addition to the reporting requirements from vendors and partners described above, DHS should provide additional auditing around these requirements and the performance of all biometric systems. DHS should aggregate these reports into one report that can be released to the public on at least an annual basis. This report should include granular data on the efficacy of biometric systems especially as it relates to persons of different demographics and similar characteristics.
- DHS should provide additional transparency around the accuracy of the biometric systems being used and specifically metrics for the types of populations that have been noted above.
- DHS should ensure that DHS Components, other government entities, partners, and vendors protect the information they are capturing. Establish data use and retention guidelines that prohibit, as appropriate, use of data beyond the purposes for which it is collected.
- CPB should train partner airlines on how to use the systems, protect information being collected and increase transparency for travelers.
- DHS should work with NIST, DHS S&T, and other academic or research organizations to ensure the most stringent algorithmic and technical standards are upheld to minimize disparity of accuracy in identification related to race, color, ethnicity, age, sex, and other similar factors.

Recommendations – Accountability & Auditing

- Continue to work with other DHS Components and Industry Stakeholders to rapidly explore new technologies in a privacy and security forward manner.
- Ensure through contractual provisions that data, images, and other information obtained through the screening of travelers is used for those limited purposes, done in a transparent manner, and subject to onward use restrictions.
- Ensure through audits that technology use limitations are enforced as well as other contractual provisions.