ABOUT FACE: EXAMINING THE DEPARTMENT OF HOMELAND SECURITY'S USE OF FACIAL RECOGNITION AND OTHER BIOMETRIC TECHNOLOGIES, PART II

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

FEBRUARY 6, 2020

Serial No. 116–60

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
41–450 PDF WASHINGTON : 2020

COMMITTEE ON HOMELAND SECURITY

Bennie G. Thompson, Mississippi, *Chairman*

Sheila Jackson Lee, Texas
James R. Langevin, Rhode Island
Cedric L. Richmond, Louisiana
Donald M. Payne, Jr., New Jersey
Kathleen M. Rice, New York
J. Luis Correa, California
Xochitl Torres Small, New Mexico
Max Rose, New York
Lauren Underwood, Illinois
Elissa Slotkin, Michigan
Emanuel Cleaver, Missouri
Al Green, Texas
Yvette D. Clarke, New York
Dina Titus, Nevada
Bonnie Watson Coleman, New Jersey
Nanette Diaz Barragán, California
Val Butler Demings, Florida

Mike Rogers, Alabama
Peter T. King, New York
Michael T. McCaul, Texas
John Katko, New York
Mark Walker, North Carolina
Clay Higgins, Louisiana
Debbie Lesko, Arizona
Mark Green, Tennessee
John Joyce, Pennsylvania
Dan Crenshaw, Texas
Michael Guest, Mississippi
Dan Bishop, North Carolina
Jefferson Van Drew, New Jersey

Hope Goins, *Staff Director*
Chris Vieson, *Minority Staff Director*

CONTENTS

Page

STATEMENTS

WITNESSES

FOR THE RECORD

ABOUT FACE: EXAMINING THE DEPARTMENT OF HOMELAND SECURITY'S USE OF FACIAL RECOGNITION AND OTHER BIOMETRIC TECHNOLOGIES, PART II

Thursday, February 6, 2020

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The committee met, pursuant to notice, at 10:05 a.m., in room 310, Cannon House Office Building, Hon. Bennie G. Thompson [Chairman of the committee], presiding.

Present: Representatives Thompson, Jackson Lee, Langevin, Payne, Rice, Correa, Small, Rose, Underwood, Slotkin, Green of Texas, Clarke, Titus, Coleman, Barragán; Rogers, McCaul, Katko, Walker, Higgins, Lesko, Green of Tennessee, Joyce, and Shaw.

Chairman THOMPSON. The Committee on Homeland Security will come to order.

Let me say at the outset a number of our Members are still en route from the Prayer Breakfast this morning, and they will join us accordingly, the Ranking Member being one of them.

The committee is meeting today to receive testimony on the Department of Homeland Security's use of facial recognition and other biometric technologies.

Without objection, the Chair is authorized to declare the committee in recess at any point.

Good morning. The committee is meeting today to continue examining the Department of Homeland Security's use of facial recognition technology.

The committee held Part I of this hearing in July of last year, after news that the Department was expanding its use of facial recognition for varying purposes, such as confirming the identity of travelers, including U.S. citizens.

As facial recognition technology has advanced, it has become the chosen form of biometric technology used by the Government and industry.

I want to reiterate that I am not wholly opposed to the use of facial recognition technology, as I recognize that it can be a valuable tool to the homeland security and serve as a facilitation tool for the Department's various missions.

But I remain deeply concerned about privacy, transparency, data security, and accuracy of this technology, and want to ensure those concerns are addressed before the Department deploys it any further.

Last July, I, along with other Members of this committee, shared these concerns at our hearings and left this room with more questions than answers.

In December 2019, the National Institute for Standards and Technology published a report that confirmed age, gender, and racial bias in facial recognition algorithms.

NIST, for example, found that depending on the algorithm, African American and Asian American faces were misidentified 10 to 100 times more than white faces.

Although CBP touts that the match rate for this facial recognition system is over 98 percent, it is my understanding that NIST did not test CBP's current algorithm for its December 2019 report.

Moreover, CBP's figures do not account for images of travelers who could not be captured due to a variety of factors, such as lighting or skin tone, actually making the actual match rate significantly lower.

These findings continue to suggest that some of this technology is not really ready for prime time and requires further testing before wide-spread deployment.

Misidentifying even a relatively small percentage of the traveling public could affect thousands of passengers annually and likely would have a disproportionate effect on certain individuals. This is unacceptable.

Data security also remains an important concern. Last year a CBP contractor experienced a significant data breach, which included traveler images being stolen.

We look forward to hearing more about these lessons CBP learned from this incident and the steps that it takes to ensure that biometric data is kept safe.

Transparency continues to be key. The American people deserve to know how the Department is collecting facial recognition data and whether the Department is, in fact, safeguarding their rights when deploying such technology.

That is why we are here 7 months later to continue our oversight. I am pleased that we again have witnesses from CBP and NIST before us to provide us with an update and answer our questions.

We will also have testimony from DHS's Office of Civil Rights and Civil Liberties. This office is charged with ensuring the protection of our civil rights and civil liberties as it relates to the Department's activities, no easy task, especially these days.

Be assured that under my leadership this committee will continue to hold the Department accountable for treating all Americans equitably and ensuring that our rights are protected.

I look forward to a robust discussion with all of the witnesses, and I thank the Members for joining us today.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

FEBRUARY 6, 2020

The Committee on Homeland Security is meeting today to continue examining the Department of Homeland Security's use of facial recognition technology. The committee held Part I of this hearing in July of last year—after news that the Department was expanding its use of facial recognition for varying purposes, such as confirming the identities of travelers, including U.S. citizens. As facial recognition technology has advanced, it has become the chosen form of biometric technology used by the Government and industry. I want to reiterate that I am not wholly opposed to the use of facial recognition technology, as I recognize that it can be valuable to homeland security and serve as a facilitation tool for the Department's varying missions. But I remain deeply concerned about privacy, transparency, data security, and the accuracy of this technology and want to ensure these concerns are addressed before the Department deploys it further.

Last July, I—along with other Members of this committee—shared these concerns at our hearing and left this room with more questions than answers. In December 2019, the National Institute for Standards and Technology (NIST) published a report that confirmed age, gender, and racial bias in some facial recognition algorithms. NIST, for example, found that depending on the algorithm, African-American and Asian-American faces were misidentified 10 to 100 times more than white faces. Although CBP touts that the match rate for its facial recognition systems is over 98 percent, it is my understanding that NIST did not test CBP's current algorithm for its December 2019 report. Moreover, CBP's figure does not account for images of travelers who could not be captured due a variety of factors such as lighting or skin tone—likely making the actual match rate significantly lower. These findings continue to suggest that some of this technology is not ready for "prime time" and requires further testing before wide-spread deployment.

Misidentifying even a relatively small percentage of the traveling public could affect thousands of passengers annually, and likely would have a disproportionate effect on certain individuals. This is unacceptable. Data security also remains an important concern. Last year, a CBP subcontractor experienced a significant data breach, which included traveler images being stolen. We look forward to hearing more about the lessons CBP learned from this incident and the steps that it has taken to ensure that biometric data is kept safe. Transparency continues to be key. The American people deserve to know how the Department is collecting facial recognition data, and whether the Department is in fact safeguarding their rights when deploying such technology. That is why we are here 7 months later to continue our oversight.

I am pleased that we again have witnesses from CBP and NIST before us to provide us with an update and answer our questions. We will also have testimony from DHS's Office for Civil Rights and Civil Liberties. This office is charged with ensuring the protection of our civil rights and civil liberties as it relates to the Department's activities—no easy task, especially these days. Be assured that under my leadership, this committee will continue to hold the Department accountable for treating all Americans equitably and ensuring that our rights are protected.

Chairman THOMPSON. Other Members are reminded that statements may be submitted for the record.

[The statement of Honorable Jackson Lee follows:]

STATEMENT OF HONORABLE SHEILA JACKSON LEE

FEBRUARY 6, 2020

Thank you, Chairman Thompson and Ranking Member Rogers for holding today's important hearing on "About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II."

I look forward to hearing from today's Government witnesses on DHS's use of facial recognition and other biometric technologies.

Good morning and welcome to our witnesses:

- Mr. John Wagner, deputy executive assistant commissioner, Office of Field Operations, U.S. Customs and Border Protection (CBP), Department of Homeland Security (DHS),
- Mr. Peter Mina, deputy officer for programs and compliance, Office for Civil Rights and Civil Liberties (CRCL), DHS,
- Dr. Charles H. Romine, director, Information Technology Laboratory, National Institute of Standards and Technology (NIST), Department of Commerce.

The hearing today provides an opportunity for Members of this committee to examine DHS's use of biometric technologies, including facial recognition technology, for Government purposes.

Biometrics is the technical term for body measurements and calculations.

It refers to metrics related to human characteristics such as fingerprints, eyes, voice, or other unique features associated with people.

Biometrics authentication is used in computer science as a form of identification and access control.

Facial recognition is one of the most popular biometrics.

Facial recognition systems are computer-based security systems, which are deployed to automatically detect and identify human faces.

Several DHS components have begun expanding their use of facial recognition technology for purposes ranging from identifying travelers to general surveillance.

My admiration and respect for the men and women of DHS as public servants who are our Nation's first line of defense against terrorism that targets our Nation is well-known.

Securing our Nation's transportation systems, critical infrastructure, and civil government agencies from cyber threats requires efficiency and effectiveness of all aspects of recruitment, training, and retention of professionals.

In the last decade, domestic terrorism has become an increasing concern in the United States, and these persons are in the United States, and not coming from overseas.

So there needs to be concern when people of color are targets of those seeking to do violence to people living within our own Nation's borders.

In 2018, domestic extremists killed at least 50 people in the United States, a sharp increase from the 37 extremist-related murders documented in 2017, though still lower than the totals for 2015 (70) and 2016 (72).

The 50 deaths made 2018 the fourth-deadliest year on record for domestic extremist-related killings since 1970.

According to an analysis by the *Washington Post,* between 2010 and 2017, right-wing terrorists committed a third of all acts of domestic terrorism in the United States (92 out of 263), more than Islamist terrorists (38 out of 263) and left-wing terrorists (34 out of 263) put together.

Recent unpublished FBI data leaked to the *Washington Post* in early March 2019 reveal that there were more domestic terrorism-related arrests than international terrorism-related arrests in both fiscal year 2017 and fiscal year 2018.

From 2009 to 2018 there were 427 extremist-related killings in the United States; of those, 73.3 percent were committed by right-wing extremists, 23.4 percent by Islamist extremists, and 3.2 percent by left-wing extremists.

In short, 3 out of 4 killings committed by right-wing extremists in the United States were committed by white supremacists (313 from 2009 to 2018).

The culmination of the 2018 mid-term election was consumed by bombs placed in the mail addressed to Democrats.

The risks posed by terrorism must be weighed aganist the privacy and civil liberties concerns raised by the deployment and use of biometric idetntification systems including facial recognition.

Today, DHS components including TSA, CBP, and ICE interact more intimately with broad swaths of the public than any other Government agency, screening over 2 million passengers every day.

On July 7, 2019, the *New York Times* reported that ICE has been mining State driver's license records for immigration purposes.

According to this article at least 3 States that offer driver's licenses to undocumented immigrants, ICE officials have requested to comb through State repositories of license photos, according to newly-released documents.

At least 2 of those States, Utah and Vermont, complied, searching their photos for matches, those records show.

In the third State, Washington, agents authorized administrative subpoenas of the Department of Licensing to conduct a facial recognition scan of all photos of license applicants, though it was unclear whether the State carried out the searches.

In Vermont, agents only had to file a paper request that was later approved by Department of Motor Vehicles employees.

Over 50 percent of all Americans are included in State Department of Motor Vehicle records.

Members of this Committee understand that several components within the Department gather and collect biometric information.

DHS uses biometrics for the purposes of identity verification, and it has looked to increase its use of technologies for such purposes.

Currently, TSA front-line workers and airline employees manually compare the traveler in front of them to the photo identification provided.

TSA seeks to leverage facial recognition technology to automate the identity verification process to enhance security effectiveness, improve operational efficiency, and streamline the traveler experience.

TSA has demonstrated an interest in using facial recognition to validate the identity of TSA PreCheck passengers who have voluntarily provided biometric information to TSA.

TSA has begun capturing photographs of passengers enrolling or renewing enrollments in PreCheck.

The U.S. Citizenship and Immigration Services (USCIS) has long collected fingerprints and pictures of applicants for immigration benefits.

CBP has begun implementing a biometric entry-exit system that relies on facial recognition for verifying a traveler's identification, including U.S. citizens.

TSA is interested in using facial recognition to validate the identity of TSA PreCheck passengers who have voluntarily provided biometric information to TSA and, eventually, to verify passenger identity for standard screening, including for domestic travel.

Beyond confirming an individual's identity, some components have been using, or are contemplating the use of, facial recognition technology to surveil a crowd of people for law enforcement purposes.

Since November, the United States Secret Service has been conducting a facial recognition pilot on a limited basis at the White House to search the faces of individuals visiting the complex or passing by on public streets and parks.

Emails from Immigration and Customs Enforcement (ICE) officials became public, which detailed meetings with Amazon over its facial recognition platform "Rekognition" and its possible use on the Southern Border.

In 2018, this same system was reported to have falsely identified 28 Members of Congress as having a match to known criminals.

The committee must fully understand the limitations of facial recognition systems.

Although algorithms may be well-developed and work extremely well, if the technology is applied to data that is of poor quality or have weak technical standards then the output can be worthless.

If the underlying technology is not the right match for the intended purpose of facial recognition or discernment then the system will fail.

The National Institute of Science (NIST) has done admirable work in producing 3 reports on the topic of facial recognition, and I look forward to learning more about their work in scoring their performance.

I gather from their efforts that they provide a technical assessment of the facial recognition applications brought to them for analysis by other Federal Government agencies.

NIST does not see the algorithms against their own data set and observe the outcomes to assess the performance of facial recognition applications.

Additionally, agency can request facial recognition for any vendor—the only requirement is that the agency wait 3 months before making a second request.

Use of facial recognition technology is expanding within and outside of the Government, which raises concerns about privacy, civil liberties, and accuracy in the application of Federal administrative procedures that may affect a range of agency decision making such as the right to travel—and extend into applications used to determine qualifications for Federal benefits programs such as Social Security, Medicare/Medicaid, or Veterans programs.

These concerns relate to the accuracy, reliability, and fairness to those who may be subject to Federal use of facial recognition systems are not trivial.

Collection and storage of facial images can occur with or without the consent of data subjects.

There is no law governing facial image capture for Government purposes.

Biometric facial recognition systems deployed at public gatherings can be used to support facial image capture for storage and later use without the knowledge or permission of data subjects.

The "one to many" application of facial recognition technology involves—taking one image of a person and comparing it to stored images of perhaps hundreds or thousands of people to successfully identify a person is the "Holy Grail" of facial recognition.

There are law enforcement, National security, defense, and homeland security applications that would benefit from the success of accurately identifying individuals.

There are also commercial applications for being able to with a high degree of accuracy pick a face out of a crowd.

Because there is such strong interest in solving the problems of face recognition the Congress does need to keep track of developments in this area.

The systems of facial recognition currently available have flaws and are not as accurate or reliable as they might become as the technology evolves.

Today, we need laws that govern how Federal biometric systems can be deployed and reign in how the data collected might be used.

The committee needs to know where DHS is getting the images it is using and whether third-party vendors allow the agency to avoid Privacy Act considerations.

It is incumbent upon our committee to provide the necessary guidance to DHS on how these technologies can be used when Constitutionally-protected activities are involved.

DHS components have proceeded with the acquisition and deployment of facial recognition technology with little guidance or oversight from the Congress or other Federal entities.

The topic of today's hearing is important and I thank the Chairman for his foresight in bringing today's witnesses before the committee.

I look forward to the testimony of today's witnesses.

Thank you.

Chairman THOMPSON. I welcome our panel of witnesses. Our first witness, Mr. John Wagner, currently serves as the deputy executive assistant commissioner for the Office of Field Operations, U.S. Customs and Border Protection. In his current role, he oversees nearly 30,000 Federal employees and manages programs related to immigration, customs, and commercial trade-related CBP missions.

Mr. Peter Mina is a deputy officer for programs and compliance at the Office of Civil Rights and Civil Liberties. Mr. Mina previously served as chief of the Labor and Employment Law Division for U.S. Immigration and Customs Enforcement.

Dr. Charles Romine is the director of the Information Technology Laboratory at the National Institute of Standards and Technology. In this position, he oversees a research program that focuses on testing and interoperability, security, usability, and reliability of information systems.

Without objection, the witnesses' full statements will be inserted in the record.

I now ask each witness to summarize his statement for 5 minutes, beginning with Mr. Wagner.

STATEMENT OF JOHN P. WAGNER, DEPUTY EXECUTIVE ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS, U.S. CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. WAGNER. Good morning. Chairman Thompson, Ranking Member Rogers, Members of the committee, thank you for the opportunity to testify here before you today on behalf of U.S. Customs and Border Protection.

I am looking forward to the opportunity to discuss the recent NIST report with you today. Since CBP is using an algorithm from one of the highest-performing vendors identified in the report, we are confident that our results are corroborated with the findings of this report.

More specifically, the report indicates while there is a wide range of performance, of the 189 different algorithms that NIST reviewed, the highest-performing algorithms had minimal to undetectable levels of demographic-based error rates.

The report also highlights some of the operational variables that impact error rates, such as gallery size, photo age, photo quality, numbers of photos of each subject in the gallery, camera quality, lighting, human behavior factors. All influence the accuracy of an algorithm.

That is why CBP has carefully constructed the operational variables in the deployment of the technology to ensure we can attain the highest levels of match rates, which remain in the 97 to 98 percent range.

One important note is that NIST did not test the specific CBP operational construct to measure the additional impact these variables may have, which is why we have recently entered into an MOU with NIST to evaluate our specific data.

But as we build out the Congressionally-mandated biometric-based entry/exit system, we are creating a system that not only meets the security mandate, but also in a way that is cost-effective, feasible, and facilitative for international travelers.

Identity requirements are not new when crossing the border or taking an international flight. Several existing laws and regulations require travelers to establish their identity and citizenship when entering and departing the United States.

CBP employs biographic and biometric-based procedures to inspect the travel documents presented by individuals to verify the authenticity of the document and determine if it belongs to the actual person presenting it.

Again, these are not new requirements. The use of facial comparison technology simply automates the process that is often done manually today.

The shortcomings of human manual review in making facial comparisons are well-documented. Humans are prone to fatigue, sometimes have biases they may not even realize to include own race and gender biases.

Fingerprint biometrics have also documented gaps in their performance. There is a small percentage of people that we see we cannot capture fingerprints from, and there are studies that document this, as well, as well as demographic correlations, most notably based on age.

We are all well aware of the issues of common names when we rely on a biographic-based vetting scheme alone. So no one system by itself is perfect.

However, since the United States, along with many other countries, put a digital photograph into the electronic chip on a passport, it would seem to make prudent sense that the technology may be useful in determination of the rightful document holder.

It is more difficult today to forge or alter a legitimate passport as security features are more stronger than they were 10 or 15 years ago, but we are still vulnerable to a person using a legitimate document, particularly a U.S. travel document, that is real but belongs to someone else.

Using facial comparison technology to date we have identified 252 imposters, to include people using 75 genuine U.S. travel documents.

The privacy continues to be integral to our biometric mission. CBP is compliant with the terms of the Privacy Act of 1974, as amended, the E-Government Act of 2002, the Homeland Security Act of 2002, the Paperwork Reduction Act of 1995, and departmental policies that govern the collection, use, and maintenance of personally-identifiable information.

CBP recently published updates to the appendices in the privacy impact assessment covering this program, and Systems of Record notices have been published on the databases to process and store the information.

We have met 3 times with representatives of the privacy advocacy community, as well as discussions with the Privacy and Civil Liberties Oversight Board, and the DHS Privacy and Integrity Advisory Committee.

In November, CBP submitted to the Office of Management and Budget a rulemaking that would solicit public comments on the proposed regulatory updates and amendments to the Federal regulations.

One final note is that our private-sector partners, the airlines and the airports, must agree to documented specific CBP business requirements if they are submitting photographs to CBP as part of this process. These requirements include a provision that images must be deleted after they are transmitted to CBP and may not be retained by the private stakeholder.

After the devastating attacks of September 11, we as a Nation asked, "How can we make sure this never happens again?" As part of that answer, the 9/11 Commission report recommended that DHS should complete as quickly as possible a biometric entry/exit screening system, and that it was, "an essential investment in National security."

CBP is answering that call in carrying out the duties Congress has given us by continuing to strengthen its biometric efforts along the travel continuum and verifying that people are who they say they are.

I thank you for the opportunity to appear today, and I look forward to your questions.

[The prepared statement of Mr. Wagner follows:]

Prepared Statement of John P. Wagner

February 6, 2020

Chairman Thompson, Ranking Member Rogers, and Members of the committee, thank you for the opportunity to testify before you on the efforts of U.S. Customs and Border Protection (CBP) to better secure our Nation by incorporating biometrics into our comprehensive entry-exit system, and to identify overstays in support of our border security mission.

CBP has received public support for its use of biometrics from the International Air Transit Association, the World Travel and Tourism Council, and the Department of Commerce Travel and Tourism Advisory Board.[1] With international air travel growing at 4.9 percent per year and expected to double by 2031, and with an increasingly complex threat posture, CBP must innovate and transform the current travel processes to handle this expanding volume. Facial comparison technology will enable CBP and travel industry stakeholders to position the U.S. travel system as best in class, in turn, driving the continued growth in air travel volume.

As authorized in several statutes and regulations, CBP is Congressionally-mandated to implement a biometric entry-exit system.[2] Prior to the *Consolidated and*

[1] International Air Transport Association, "Resolution: End-to-end Seamless Travel across Borders Closer to Reality" (June 2, 2019). *www.iata.org/en/pressroom/pr/2019-06-02-06/*. World Travel & Tourism Council, "Gloria Guevara: 'We must act and assign priority and resources to biometrics'". March 6, 2019. *www.wttc.org/about/media-centre/press-releases/press-releases/2019/we-must-act-and-assign-priority-and-resources-to-biometrics/*. United States Travel and Tourism Advisory Board, letter to Commerce Secretary, Wilbur Ross, containing challenges and recommendation on U.S. Government-private industry partnerships on biometric technology (April 29, 2019). *https://legacy.trade.gov/ttab/docs/TTAB__Biometrics%20Recommendations%20Letter__042919.pdf*.

[2] Statutes that require DHS to take action to create an integrated entry-exit system: Sec. 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), P.L. 106–215, 114 Stat. 337; Sec. 110 of the Illegal Immigration Reform and Immigrant

Further Continuing Appropriations Act of 2013 (Public Law 113–6), which transferred the biometric exit mission from the Department of Homeland Security's (DHS) United States Visitor and Immigration Status Indicator Technology (US–VISIT) Program within the National Protection and Programs Directorate (NPPD) to CBP, the U.S. Government and the private sector were developing independent biometrics-based schemes for administering the entry-exit program responsibilities. These varied and often uncoordinated investments relied on multiple biometrics and required complicated enrollment processes. Public and private-sector entities developed separate uses for biometrics, each with varying privacy risks and accountability mechanisms. In 2017, CBP developed an integrated approach to the biometric entry-exit system that other U.S. Government agencies with security functions, such as TSA, as well as travel industry stakeholders such as airlines, airports, and cruise lines, could incorporate into their respective mission space.

CBP offered relevant stakeholders an "identity as a service" solution that uses facial comparison to automate manual identity verification, thereby harmonizing the data collection and privacy standards each stakeholder must follow. This comprehensive facial comparison service leverages biographic and biometric data, both of which are key to support CBP's mission, to fulfill the Congressional biometric entry-exit mandate while using the system to support air travel, improve efficiency, and increase the efficacy of identity verification. CBP has been testing options to leverage biometrics at entry and departure, specifically through the use of facial comparison technology.[3] These technologies enhance the manual process used today by making it more efficient, accurate, and secure. Using data that travelers are already required by statute to provide, the automated identity verification process uses facial comparison to identify those who are traveling on falsified or fraudulent documents as well as those seeking to evade screening. These are the individuals who present public safety or National security threats or have overstayed their authorized period of admission.

PREVIOUS EFFORTS TO LAUNCH A BIOMETRIC EXIT SYSTEM

Prior to the *Consolidated and Further Continuing Appropriations Act of 2013* (Public Law 113–6), which transferred the biometric exit mission from DHS headquarters to CBP, the U.S. Government and the private sector were already developing independent biometric solutions for administering entry-exit programs. For example, from January 2004 through May 2007, DHS placed kiosks between security checkpoints and airline gates to collect travelers' fingerprint biometrics. The traveler had the responsibility to find and use the devices, while airports where the kiosks were deployed provided varying degrees of support. In 2008, DHS issued a Notice of Proposed Rulemaking (NPRM) that proposes commercial air and vessel carriers collect biometric information from certain aliens departing the United States and submit this information to DHS within a certain time frame. Most comments opposed the adoption of the proposed rule, citing cost and feasibility. Among other comments was the suggestion that biometrics collection should strictly be a Governmental function. The suggestion was made that the highly competitive air industry could not support a major new process of biometric collection on behalf of the Government, and that requiring air carriers to collect biometrics was not feasible and would unfairly burden air carriers and airports. Additionally, as directed by Congress, from May through June 2009, DHS operated 2 biometric exit pilot programs in which CBP used a mobile device to collect biometric exit data at departure gates while TSA collected it at security checkpoints.

DHS concluded from the NPRM comments and pilot programs that it was generally inefficient and impractical to introduce entirely new Government processes into an existing and familiar traveler flow, particularly in the air environment. DHS also concluded that the use of mobile devices to capture electronic fingerprints

Responsibility Act of 1996, P.L. 104–208, 110 Stat. 3009–546; Sec. 205 of the Visa Waiver Permanent Program Act of 2000, P.L. 106–396, 114 Stat. 1637, 1641; Sec. 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), P.L. 107–56, 115 Stat. 272, 353; Sec. 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), P.L. 107–173, 116 Stat. 543, 552; Sec. 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), P.L. 108–458, 118 Stat. 3638, 3817; Sec.711 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110–53, 121 Stat. 266, 338; and Sect. 802 of the Trade Facilitation and Trade Enforcement Act of 2015, P.L. 114–125, 130 Stat. 122, 199. In addition, through the Consolidated Appropriations Act of 2016 and the Bipartisan Budget Act of 2018, Congress authorized up to $1 billion in visa fee surcharges through 2027 to support biometric entry/exit. P.L. 114–113 129 Stat. 2242 (December 17, 2015); P.L. 115–123 132 Stat. 64 (February 9, 2018).

[3] DHS/CBP (November 2018), *DHS/CBP/PIA–056 Traveler Verification Service.* (945.31 KB).

would be extremely resource-intensive. This information helped frame our concept for a comprehensive biometric entry-exit system that would avoid adding new processes; utilize existing infrastructure; leverage existing stakeholder systems, processes, and business models; leverage passenger behaviors and expectations; and utilize existing traveler data and existing Government information technology infrastructure.

CBP'S INTEGRATED APPROACH TO A COMPREHENSIVE BIOMETRIC ENTRY-EXIT SYSTEM

Leveraging CBP's current authorities, we are executing Congressional mandates to create and test an integrated biometric entry-exit system using facial comparison technology. This technology uses existing advance passenger information along with photographs already provided to the Government by international travelers to create "galleries" of facial image templates that correspond with the individuals expected on international flights arriving or departing the United States. These photographs may be derived from passport applications, visa applications, or interactions with CBP at a prior border inspection.[4] Once the gallery is created based on the advance information, the biometric comparison technology compares a template of a live photograph of the traveler—taken where there is clear expectation and authority that a person will need to provide documentary evidence of their identity—to the gallery of facial image templates.

For technical demonstrations at the land border, air entry, and some air exit operations, CBP cameras take photographs of travelers. These tests have been extended on a voluntary basis to exempt certain aliens and U.S. citizens.[5] Participation provides a more accurate and efficient method to verify identity and citizenship. In other air exit and seaport demonstrations, CBP does not take the photographs. Instead, specified partners, such as commercial air carriers, airport authorities, and cruise lines, take photographs of travelers and transmit the images to CBP's facial matching service. These partners use their own camera operators and technology that meets CBP's technical and security requirements. These tests occur on a voluntary basis and are consistent with that partner's contractual relationship with the traveler.

Biometric entry-exit is not a surveillance program. CBP does not use hidden cameras. CBP uses facial comparison technology to ensure a person is who they say they are—the bearer of the passport they present. This technology provides a seamless way for in-scope travelers to meet the requirement to provide biometrics upon departure from the United States. Travelers are aware their photos are being taken and that they can opt out as described below. CBP uses facial comparison technology only where a current identity check already exists. CBP works closely with partner air carriers and airport authorities to post privacy notices and provide tear sheets for impacted travelers and members of the public in close proximity to the cameras and operators, whether the cameras are owned by CBP or the partners.

The imposter threat—or the use of legitimate documents that do not belong to the bearer—continues to be a challenge for CBP. U.S. passports are the most prized version of an imposter document because—until recently—there was no biometric comparison between the person presenting the document and the owner of the document. As document security standards have increased in the past 20 years, it has become much more difficult to plausibly forge or alter a legitimate document. As a result, those who wish to evade detection seek to use legitimate documents that belong to someone else. U.S. citizens are not required to provide fingerprint biometrics for entry into the country whereas foreign nationals may be required to do so.

[4] Department of State, Consular Consolidated System, "Privacy Impact Assessment: Consular Consolidated Database" (January 29, 2020). *https://2001-2009.state.gov/documents/organization/93772.pdf.*

[5] Under Scope of examination, Alien applicants for admission, 8 C.F.R. § 235.1(f)(1)(ii) and Requirements for biometric identifiers from aliens on departure from the United States, 8 C.F.R. § 215.8(a)(1), CBP may require certain aliens to provide biometric identifiers to confirm their admissibility or, at specified airports, their departure. Some aliens are exempt from the requirement to provide biometrics. This includes Canadians, under Sect.101(a)(15)(B), who are not otherwise required to present a visa or be issued a Form I–94 or Form I–95; aliens younger than 14 or older than 79 on the date of admission; aliens admitted A–1, A–2, C–3 (except for attendants, servants, or personal employees of accredited officials), G–1, G–2, G–3, G–4, NATO–1, NATO–2, NATO–3, NATO–4, NATO–5, or NATO–6 visas; and certain Taiwan officials and members of their immediate families who hold E–1 visas, unless the Secretary of State and the Secretary of Homeland Security jointly determine that a class of such aliens should be subject to the requirements of paragraph (d)(1)(ii); classes of aliens to whom the Secretary of Homeland Security and the Secretary of State jointly determine the requirement shall not apply; or an individual alien to whom the Secretary of Homeland Security, the Secretary of State, or the Director of Central Intelligence determines this requirement shall not apply.

CBP is authorized to require "in-scope" aliens to provide biometric identifiers.[6] For entry, CBP uses cameras and facial comparison technology during the inspection process. CBP operates facial comparison technology pilots at exit in certain land and sea ports and some airports.[7] This technology provides the travel industry with the tools to verify traveler identity and transmit information to CBP.[8] We have identified best practices from the prior DHS work as well as from our international partners and used them in the biometric exit system design to avoid an inefficient two-step process that requires multiple biometrics to verify traveler identity.

CBP understood the need to build a system that all stakeholders within the travel continuum could participate in without building their own independent system—one that could expand to other mission areas outside of the biometric exit process. To address these challenges and satisfy the Congressional mandate, we are working closely with our partners to integrate biometrics with existing identity verification requirements to the extent feasible.[9] Facial comparison technology can match more than 97 percent of travelers through the creation of facial galleries.[10] The match rate is based on the percentage of travelers with a valid encounter photo who were successfully matched to a gallery photo.[11]

While CBP's primary responsibility is National security, we must also facilitate legitimate trade and travel. The use of facial comparison technology has enabled CBP to not only address a National security concern head-on by enhancing identity verification but to simultaneously improve the traveler experience throughout the travel continuum. CBP engineered a biometric exit solution that gives not only CBP, but TSA and industry stakeholders such as airlines and airports, the ability to automate manual identity verification. This may include departure gates, debarkation (arrival) areas, airport security checkpoints, and Federal Inspection Services areas.

CBP uses only photos collected from cameras deployed specifically for this purpose and does not use photos obtained from closed-circuit television or other live or recorded video. As the facial comparison technology automates the manual identity verification process in place today, it allows CBP and its stakeholders to make quicker and more informed decisions. In August 2019, CBP and TSA provided this committee a comprehensive report on the program that included material on the operational and security benefits of the biometric entry-exit system, CBP and TSA's efforts to address privacy concerns and potential performance differential errors, and a comprehensive description of audits performed.[12]

CBP AUTHORITIES

As described above, numerous Federal statutes require DHS to create an integrated, automated biometric entry and exit system that records the arrival and departure of aliens, compares the biometric data to verify their identities, and authenticates travel documents. Most recently, in 2017, Executive Order 13780 called for the expedited completion of the biometric entry-exit data system.[13] DHS has broad

[6] "In scope" aliens may be required to provide biometric identifiers to confirm their admissibility, or, at specified airports, their departure in accordance with Inspection of Persons Applying for Admission, Scope of examination, Alien applicants for admission, 8 C.F.R. § 235.1(f)(1)(ii) and Requirements for biometric identifiers from aliens on departure from the United States, 8 C.F.R. § 215.8(a)(1).

[7] Requirements for biometric identifiers from aliens on departure from the United States, 8 C.F.R. § 215.8(a)(1).

[8] Numerous statutes require advance electronic transmission of passenger and crew member manifests for commercial aircraft and commercial vessels. These mandates include, but are not limited to Sec. 115 of the Aviation and Transportation Security Act (ATSA), P.L. 107–71, 115 Stat. 597; Passenger manifests, 49 U.S.C. § 44909 (applicable to passenger and crew manifests for flights arriving in the United States); Sec. 402 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSVERA), P.L. 107–173, 116 Stat. 543; List of alien and citizen passengers arriving and departing, 8 U.S.C. § 1221; and Examination of merchandise, 19 U.S.C. § 1499.

[9] Ibid.

[10] Department of Homeland Security Fiscal Year 2018 Entry/Exit Overstay Report, *https://www.dhs.gov/sites/default/files/publications/19_0417_fy18-entry-and-exit-overstay-report.pdf.*

[11] DHS/CBP (November 2018), DHS/CBP/PIA–056 Traveler Verification Service. (945.31).

[12] DHS, "Transportation Security Administration and Customs and Border Protection: Deployment of Biometric Technologies, Report to Congress" (August 30, 2019 *www.tsa.gov/sites/default/files/biometricsreport.pdf.*

[13] Other statues that require DHS to create an integrated entry-exit system include: Sect. 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), P.L. 106–215, 114 Stat. 337; Sec. 205 of the Visa Waiver Permanent Program Act of 2000, P.L. 106–396, 114 Stat. 1637, 1641; and Sec. 414 of the Uniting and Strengthening Amer-

Continued

authority to control alien travel and to inspect aliens under various provisions of the Immigration and Nationality Act of 1952 (INA), as amended.[14] As part of CBP's authority to enforce U.S. immigration laws, CBP is responsible for interdicting individuals illegally entering or exiting the United States; facilitating and expediting the flow of legitimate travelers; and detecting, responding to, and interdicting terrorists, drug smugglers, human smugglers, traffickers, and other persons who may undermine the security of the United States at entry.

To effectively carry out its responsibilities under the INA for both arrivals and departures from the United States, CBP must be able to conclusively determine if a person is a U.S. citizen or national or an alien by verifying that the person is the true bearer of his or her travel documentation. CBP is authorized to take and consider evidence concerning the privilege of any person to enter, reenter, pass through, or reside in the United States, or concerning any matter material or relevant to the enforcement or administration of the INA.[15] A person claiming U.S. citizenship must establish that fact to the examining officer's satisfaction and must present a U.S. passport or alternative documentation.[16]

To further advance the legal framework, CBP is working to propose and implement regulatory amendments. CBP is working on a biometric entry/exit regulation, which will only impact foreign nationals. In November 2019, CBP transmitted its proposed regulation on biometric entry/exit to the Office of Management and Budget; we are awaiting clearance. The rule will go through the full rulemaking process, which includes a public comment period.

NIST FACIAL COMPARISON VENDOR TEST: DECEMBER 2019

CBP has partnered with the National Institute of Standards and Technology (NIST) to explore facial comparison technology capabilities. NIST used CBP data that was contained in the OBIM data in its conclusions issued in a recent demographic differential study. The study supports what CBP has seen in its biometric matching operations—that when a high-quality facial comparison algorithm is used along with high-performing cameras, proper lighting and image quality controls, face-matching technology can be highly accurate. To ensure higher accuracy rates, as well as efficient traveler processing, CBP compares traveler photos to a very small gallery of high-quality images that those travelers already provided to the U.S. Government to obtain a passport or visa.

CBP uses only one of the 189 face comparison algorithms evaluated by NIST and produced by NEC Corporation. As the report demonstrates, NIST confirmed that the NEC algorithm that NIST tested is high-performing and ranked first or second in most categories evaluated, including match performance in galleries that are much bigger than those used by CBP.[17] The NIST performance metrics described in the report are consistent with CBP operational performance metrics for entry-exit. CBP's operational data continues to show there is no measurable differential performance in matching based on demographic factors. The NIST report shows a wide range in accuracy across algorithm developers, with the most accurate algorithms

ica by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), P.L. 107–56, 115 Stat. 272, 353.

[14] Biometric entry and exit data system, 8 U.S.C. § 1365b mandates the creation of an integrated and comprehensive system. The entry and exit data system shall include a requirement for the collection of biometric exit data for all categories of individuals required to provide biometric entry data. As a result, if a certain category of individuals is required to provide biometrics to DHS on entry as part of the examination and inspection process, the same category of individuals must be required to provide biometrics on exit as well. DHS may require individuals to provide biometrics and other relevant identifying information upon entry to, or departure from, the United States. Specifically, DHS may control alien entry and departure and inspect all travelers under § § 215(a) and 235 of the INA (8 U.S.C. § 1185, 1225). Aliens may be required to provide fingerprints, photographs, or other biometrics upon arrival in, or departure from, the United States, and select classes of aliens may be required to provide information at any time. See, e.g., INA 214, 215(a), 235(a), 262(a), 263(a), 264(c), (8 U.S.C. 1184, 1185(a), 1225(a), 1302(a), 1303(a), 1304(c)); 8 U.S.C. § 1365b. Pursuant to § 215(a) of the INA (8 U.S.C. § 1185(a)), and Executive Order No. 13323 (December 30, 2003) (69 FR 241), the Secretary of Homeland Security, with the concurrence of the Secretary of State, has the authority to require aliens to provide requested biographic information, biometrics, and other relevant identifying information as they depart the United States.

[15] Powers of immigration officers and employees, 8 U.S.C. § 1357(b).

[16] Under Scope of examination, 8 C.F.R. § 235.1(b), it is generally unlawful for a U.S. citizen to depart or attempt to depart from the United States without a valid passport. See also Travel control of citizens and aliens, 8 U.S.C. § 1185(b); and Passport requirement; definitions, 22 C.F.R. § 53.1.

[17] Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects, National Institute of Standards and Technology, U.S. Department of Commerce (December 2019), p.8.

producing many fewer errors and undetectable false positive differentials. Since many of the performance rates specified in the report would not be acceptable for use in CBP operations, we do not use them.

CBP is committed to implementing the biometric entry exit mandate in a way that provides a secure and streamlined travel experience for all travelers, and CBP will continue to partner with NIST and use NIST research to ensure the continued optimal performance of the CBP face comparison service. In the upcoming weeks, CBP will directly provide NIST with data for NIST to perform an independent and comprehensive scientific analysis of CBP's operational face-matching performance, including impacts due to traveler demographics and image quality. NIST will provide objective recommendations regarding matching algorithms, optimal thresholds, and gallery creation.

DATA SECURITY

There are 4 primary safeguards to secure passenger data, including secure encryption during data storage and transfer, irreversible biometric templates, brief retention periods, and secure storage. Privacy is implemented by design, ensuring data protection through the architecture and implementation of the biometric technology. CBP prohibits its approved partners such as airlines, airport authorities, or cruise lines from retaining the photos they collect as part of the entry/exit program for their own business purposes. The partners must immediately purge the images following transmittal to CBP, and the partner must allow CBP to audit compliance with this requirement. As discussed in its comprehensive November 2018 Privacy Impact Assessment concerning its facial recognition technology, CBP has developed business requirements, or system-wide standards, to document this commitment.[18] Our private-sector partners must agree as a condition of participation in the pilots.

PRIVACY, TRANSPARENCY, CIVIL RIGHTS, AND FUTURE ASSESSMENTS

CBP is committed to ensuring that our use of technology sustains and does not erode privacy protections. We take privacy very seriously and are dedicated to protecting the privacy of all travelers. CBP complies with the requirements of the *Privacy Act of 1974* and all DHS and Government-wide policies.[19] In accordance with DHS policy, CBP uses the Fair Information Practice Principles, or FIPPs, to assess the privacy risks and ensure appropriate measures are taken to mitigate risks from data collection through the use of biometrics. Our partnering stakeholders are also held to the same standards.

CBP strives to be transparent and provide notice to individuals regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). When airlines or airports partner with CBP on biometric air exit, the public is informed that the partner is collecting the biometric data in coordination with CBP. We notify travelers at these ports using verbal announcements, signs, and/or message boards that CBP takes photos for identity verification purposes, and they are informed of their ability to opt out. Foreign nationals may opt out of providing biometric data to a third party, and any U.S. citizen or foreign national may do so at the time of boarding by notifying the airline-boarding agent that they would like to opt out. The airline would conduct manual identity verification using their travel document, and may notify CBP to collect biometrics, if applicable.

If requested, CBP Officers provide a tear sheet with Frequently Asked Questions, opt-out procedures, and additional information, including the legal authority and purpose for inspection, the routine uses, and the consequences for failing to provide information. CBP also posts signs informing individuals of possible searches, and the purpose for those searches, upon arrival or departure from the United States. CBP provides general notification of its biometric exit efforts and various pilot programs through Privacy Impact Assessments (PIAs) and Systems of Records Notices (SORNs) and through information such as Frequently Asked Questions, which are readily available at *www.cbp.gov.*[20]

CBP published a comprehensive PIA concerning its facial recognition technology, known as the Traveler Verification Service, in November 2018. An appendix to that document, published on January 8, 2020, explains aspects of CBP's biometric use as well as policies and procedures for the collection, storage, analysis, use, dissemi-

[18] DHS/CBP (November 2018), *DHS/CBP/PIA–056 Traveler Verification Service.* (945.31 KB).

[19] Records maintained on individuals, 5 U.S.C. § 552(a), P.L. 93–579, 88 Stat. 1896.

[20] SORNs associated with CBP's Traveler Verification Service are: DHS/CBP–007 Border Crossing Information, DHS/CBP–021 Arrival and Departure Information System, DHS/CBP–006 Automated Targeting System, DHS/CBP–011 U.S. Customs and Border Protection TECS. *https://www.dhs.gov/system-records-notices-sorns.*

nation, retention, and/or deletion of data.[21] The PIA and the public notices specifically highlight that facial images for arriving and departing foreign nationals (and those dual national U.S. citizens traveling on foreign documentation) are retained by CBP for up to 2 weeks, not only to confirm travelers' identities but also to assure continued accuracy of the algorithms and ensure there are no signs of any differential performance. As always, facial images of arriving and departing foreign nationals are forwarded to the IDENT system for future law enforcement purposes, consistent with CBP's authority. As U.S. citizens are not within the scope for biometric exit, photos of U.S. citizens used for biometric matching purposes are held in secure CBP systems for no more than 12 hours after identity verification in case of an extended system outage or for disaster recovery.[22] CBP reduced the retention period for U.S. citizen photos to no more than 12 hours as a direct result of briefings and consultations with Chairman Thompson.

CBP is committed to transparency in this process as well as to improving its public messaging to help the public better understand the technology. We welcome the committee's input. CBP collaborates regularly with the DHS Privacy Office to ensure compliance with privacy laws and policies. The DHS Privacy Office commissioned the DHS Data Privacy and Integrity Advisory Committee (DPIAC) to advise the Department on best practices for the use of facial comparison technology. The DPIAC published its report on February 26, 2019.[23] CBP has implemented or is actively working to implement all of the DPIAC recommendations. CBP continues outreach efforts with privacy advocacy groups regarding the biometric entry-exit program, most recently meeting with them in December 2019. CBP also hosted the Privacy and Civil Liberties Oversight Board (PCLOB) for a tour of biometric processes at Atlanta/Hartsfield International Airport on January 15, 2020.[24]

CBP'S PROGRESS TOWARD IMPLEMENTING A COMPREHENSIVE BIOMETRIC ENTRY-EXIT SYSTEM

Biometric Entry-Exit in the Air Environment

Facial comparison technology is enhancing the arrivals process, enabling more efficient and more secure clearance processes that benefit airports, airlines, and travelers with shorter connection times and standardized arrival procedures. It is an additional tool to reduce imposter threat while increasing the integrity of the immigration system. Since initiating the use of facial comparison technology in the air environment on a trial basis, CBP has identified 7 imposters, including 2 with genuine U.S. travel documents (passport or passport card), using another person's valid travel documents to seek entry into the United States.[25]

CBP is working toward full implementation of biometric exit in the air to account for over 97 percent of departing commercial air travelers from the United States. Stakeholder partnerships are critical for implementing a biometric entry-exit system, and airports, airlines, and CBP are collaborating to develop a process that meets our biometric entry-exit mandate and airlines' business needs. These partnerships help ensure that biometric entry-exit does not have a detrimental impact on the air travel industry, and that the technology is useful and affordable. Stakeholders have attested that using biometrics could lead to faster boarding times, enhanced customer service, better use of our CBP staffing, and faster flight clearance times on arrival. Engagement with additional stakeholders on how they can be incorporated into the comprehensive entry-exit system continues, and CBP is ready to partner with any appropriate airline or airport that wishes to use biometrics to expedite the travel process for its customers.

Biometric Entry-Exit in the Land Environment

In the land environment, there are often geographical impediments to expanding exit lanes to accommodate adding lanes or CBP-staffed booths. The biometric exit land strategy focuses on implementing an interim exit capability while simulta-

[21] DHS/CBP (November 2018), DHS/CBP/PIA–056 Traveler Verification Service. (945.31 KB).

[22] Controls of aliens departing from the United States; Electronic visa update system, 8 C.F.R. § 215; Inspection of persons applying for admission, 8 C.F.R. § 235.

[23] Report 2019–01 of the DHS Data Privacy and Integrity Advisory Committee (DPIAC): Privacy Recommendations in Connection with the Use of Facial Recognition Technology, *Privacy Recommendations in Connection with the Use of Facial Recognition Technology.pdf.*

[24] The Privacy Civil Rights Oversight Board is an independent, bipartisan agency within the Executive branch established by the Implementing Recommendations of the 9/11 Commission Act, P.L. 110–53, *https://www.pclob.gov/*. Nextgov, Inside the CBP-Build 'Backbone' of Atlanta's Biometric Terminal, (January 21, 2020) *inside-cbp-built-backbone-atlantas-biometric-terminal.*

[25] Updated January 7, 2020.

neously investigating what is needed to implement a comprehensive system over the long term. Biometrically verifying travelers who depart at the land border will close a gap in the information necessary to complete a nonimmigrant traveler's record in CBP's Arrival and Departure Information System, and will allow us an additional mechanism to better determine when travelers who depart the United States via land have overstayed their admission period. Given DHS's desire to implement the use of biometrics without negatively affecting cross-border commerce, CBP plans to take a phased approached to land implementation.

Facial comparison technology, similar to what is used in the air environment has been deployed at entry operations at the Nogales and San Luis POEs in Arizona and at the Laredo and El Paso POEs in Texas. CBP plans to expand to additional locations along the Southern Border in 2020. By using the facial comparison technology in the land environment, CBP has identified 247 imposters, including 45 with criminal records and 18 under the age of 18, attempting to enter the United States. Additionally, CBP tested "at speed" facial biometric capture camera technology on vehicle travelers.[26] From August 2018 to February 28, 2019, CBP conducted a technical demonstration on people inside vehicles moving less than 20 miles per hour entering and departing Anzalduas, Texas.

Biometric Entry-Exit in the Sea Environment

Similar to efforts in the air environment, CBP is partnering with the cruise line industry to use facial biometric processing supported by CBP's biometric comparison service in the debarkation points at seaports.[27] Automating identity verification allows us to shift officer focus to core law enforcement functions and reallocate resources from primary inspections to roving enforcement activities. Currently, there are 7 sea entry sites and 5 major cruise lines that are operating facial comparison cameras to confirm arriving passenger identity on closed-loop cruises, which begin and end in the same city. Cruise lines report passenger satisfaction feedback that indicate the debarkation process is significantly better than feedback from vessels not using the technology during debarkation. CBP continues engagement with cruise lines and port authorities to expand the technology to other businesses and locations.

CONCLUSION

DHS, in collaboration with the travel industry, is assertively moving forward in developing a comprehensive biometric exit system in the land, air, and sea environments that replace manual identity checks with facial comparison technology. Travelers are well aware that their picture is being taken for facial comparison purposes, and they have access to both basic and detailed information regarding CBP's collection of biometric information. Not only is CBP Congressionally-mandated to implement a biometric entry-exit system, such a system will enhance CBP's ability to accomplish its mission: To safeguard America's borders thereby protecting the public from dangerous people and materials while enhancing the Nation's global economic competitiveness by enabling legitimate trade and travel. CBP's collaborative biometric efforts address the recommendations of The 9/11 Commission Report, specifically, that security and protection should be shared among the various travel checkpoints (ticket counters, gates, and exit controls): "By taking advantage of them all, we need not depend on any one point in the system to do the whole job."[28]

Chairman THOMPSON. Thank you for your testimony.

I now recognize Mr. Mina to summarize his statement for 5 minutes.

STATEMENT OF PETER E. MINA, DEPUTY OFFICER FOR PROGRAMS AND COMPLIANCE, OFFICE OF CIVIL RIGHTS AND CIVIL LIBERTIES, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. MINA. Good morning. Chairman Thompson, Ranking Member Rogers, and distinguished Members of the committee, thank you for the opportunity to appear before you today to discuss the

[26] DHS/CBP (November 2018), DHS/CBP/PIA–056 Traveler Verification Service (945.31 KB).
[27] Ibid.
[28] The 9/11 Commission, *The 9/11 Commission Report,* pp. 385–386, *http://govinfo.library.unt.edu/911/report/911Report.pdf.* (7.22MB).

Department of Homeland Security's use of facial recognition technology.

DHS's commitment to nondiscrimination in law enforcement and screening activities remains an important cornerstone of our daily work to secure the homeland.

I would like to make 3 overarching points in my testimony today.

First, the Office of Civil Rights and Civil Liberties has been and continues to be engaged with the DHS operational components to ensure use of facial recognition technology is consistent with civil right and civil liberties, law, and policy.

Second, operators, researchers, and civil rights policy makers must work together to prevent algorithms from leading to impermissible biases in the use of facial recognition technology.

Third, facial recognition technology can serve as an important tool to increase the efficiency and effectiveness of the Department's public protection mission, as well as the facilitation of lawful travel.

But it is vital that these programs utilize technology in a way that safeguards our Constitutional rights and values.

Now, to achieve these 3 points, CRCL, No. 1 influences DHS policies and programs throughout their life cycle.

No. 2, engages with Department offices and components in the development of new policies and programs to ensure that protection of civil rights and civil liberties is fully integrated into their foundation.

No. 3, monitors operational execution and engages with stakeholders in order to provide feedback regarding the impacts and consequences of policies and programs.

Fourth and finally, we investigate complaints and make recommendations to DHS components, such as complaints including allegations of racial profiling or other impermissible bias.

CRCL recognizes the potential risks of impermissible bias in facial recognition algorithms, as previously raised by this committee, and supports rigorous testing and evaluation of algorithms used in facial recognition systems to identify and mitigate impermissible bias.

CRCL will continue to support the collaborative relationship between the National Institute of Standards and Technology, the DHS Science and Technology Directorate, the DHS Office of Biometric and Identity Management, and DHS components, including U.S. Customs and Border Protection, to that end.

In carrying out its mission, CRCL advised DHS components and Department offices by participating in enterprise-level groups working on biometric and facial recognition issues.

Further, CRCL directly engages with DHS components. For example, CRCL has regularly engaged CBP on the implementation of facial recognition technology and its biometric entry and exit program.

In particular, CRCL advised on policy and implementation of appropriate accommodations for individuals wearing religious headwear, for individuals with a sincere religious objection to being photographed, and for individuals who may have a significant injury or disability for whom taking photographs may present challenges or not be possible.

As DHS's facial recognition program has matured and evolved, CRCL will be collaborating directly with CBP, S&T, and OBIM to address potential civil rights and civil liberties impacts.

Further, CRCL will engage communities with CBP and DHS S&T to both inform the public regarding CBP's facial recognition programs and address potential concerns.

Finally, we will continue to evaluate any potential alleged violations of civil rights or civil liberties in order to further inform our policy advice and strengthen DHS's facial recognition programs.

CRCL understands that successful and appropriate facial recognition technology requires on-going oversight and quality assurance, initial validation and regular revalidation, and a close relationship between the users and oversight offices.

In this way it can be developed to work properly and without impermissible bias when it achieves initial operating capability and then continually throughout its entire project life cycle.

At the same time, we will need to work with the operational components to ensure that policies and practices evolve so that the human part of the equation, the users, are also focused on responsible deployment of this technology, working in a manner that prevents impermissible bias in DHS activities.

Again, I thank you for the opportunity to appear before you today, and I look forward to answering your questions.

[The prepared statement of Mr. Mina follows:]

Prepared Statement of Peter E. Mina

February 6, 2020

Chairman Thompson, Ranking Member Rogers, and distinguished Members of the committee, thank you for the opportunity to appear before you to discuss the Department of Homeland Security's (DHS) use of facial recognition technology. DHS's commitment to nondiscrimination in law enforcement and screening activities remains an important cornerstone of our daily work to secure the homeland.

I would like to make three overarching points in my testimony today: (1) The Office for Civil Rights and Civil Liberties (CRCL) has been and continues to be engaged with the DHS operational components to ensure use of facial recognition technology is consistent with civil rights and civil liberties law and policy; (2) operators, researchers, and civil rights policy makers must work together to prevent algorithms from leading to racial, gender, or other impermissible biases in the use of facial recognition technology; and (3) facial recognition technology can serve as an important tool to increase the efficiency and effectiveness of the Department's public protection mission, as well as the facilitation of lawful travel, but it is vital that these programs utilize this technology in a way that safeguards our Constitutional rights and values. To that end, we welcome the opportunity to work with DHS policy makers and operators, Congress, academic, and other non-Governmental entities on these important issues.

INTRODUCTION

CRCL supports the DHS mission to secure the Nation while preserving individual liberty, fairness, and equality under the law. Established by the Homeland Security Act of 2002, CRCL's mission integrates civil rights and civil liberties into all DHS activities by:

- Promoting respect for civil rights and civil liberties in policy development and implementation by advising Department leadership and personnel, and State and local partners;
- Communicating with individuals and communities whose civil rights and civil liberties may be affected by Department activities, informing them about policies and avenues of remedy, and promoting appropriate attention within the Department to their experiences and concerns;

- Investigating and resolving civil rights and civil liberties complaints filed by the public regarding Department policies or activities, or actions taken by Department personnel; and
- Leading the Department's equal employment opportunity programs and promoting workforce diversity and merit system principles.

CRCL is a DHS headquarters office, and the CRCL officer reports directly to the Secretary of Homeland Security. CRCL works collaboratively with, but independently of, the DHS operational components, including U.S. Customs and Border Protection (CBP). CRCL's work is not, with limited but important exceptions,[1] remedial in nature.

Pursuant to statutory authorities under 6 U.S.C. § 345 and 42 U.S.C. § 2000ee–1, CRCL is responsible for assisting the Department in developing, implementing, and periodically reviewing policies and procedures to ensure the protection of civil rights and civil liberties, including in CBP and other component screening and vetting programs.

In carrying out its statutory mission, CRCL influences DHS policies and programs throughout their life cycle. CRCL seeks to engage with Department offices and components in the development of new policies and programs to ensure that protection of civil rights and civil liberties are fully integrated into their foundations. As implementation begins, CRCL monitors operational execution and engages with stakeholders in order to provide feedback to Department and component leadership regarding the impacts or consequences of policies and programs. Finally, CRCL investigates complaints and makes recommendations to DHS components, often related to the creation or modification of policies, or changes to implementation, training, supervision, or oversight. Such complaints include allegations of racial profiling or other impermissible bias. It is important to note that the DHS Office of Inspector General has the right of first refusal to investigate allegations submitted to CRCL.

DHS'S USE OF FACIAL RECOGNITION TECHNOLOGY AND CRCL'S ROLE IN OVERSIGHT

DHS currently uses facial recognition technology to support CBP's Biometric Entry-Exit Program and is researching and testing this technology to see if it can be deployed in other mission areas, such as identity verification in Transportation Security Administration passenger screening. A key goal of the Department's use of facial recognition technology is identifying and eliminating, to the extent it exists, any impermissible bias based on race and gender. In addition to the strong civil rights and civil liberties interest in ensuring equality of treatment, the DHS operational components have a compelling interest in ensuring the accuracy of this or any tool that assists in performing the mission. Improved accuracy and efficiency in the Department's data systems results in better performance of all the DHS missions they support.

DHS partnered with the National Institute of Standards and Technology (NIST) on the assessment of facial recognition technologies to improve data quality and integrity, and ultimately the accuracy of the technology, as a means of eliminating such impermissible bias.

- Currently, the DHS Office of Biometric Identity Management (OBIM) is partnering with NIST to develop a face image quality standard that will improve the accuracy and reliability of facial recognition as it is employed at DHS.
- CBP is partnering with NIST to analyze performance impacts due to image quality and traveler demographics and providing recommendations regarding match algorithms, optimal thresholds for false positives, and the selection of photographs used for comparison.

DHS knows that accuracy and reliability, and the resulting operational value of facial recognition technology, varies depending on how the technology is employed. Variables include the nature of the mission supported, variations in the type and quality of the photographs, environmental factors such as lighting, the manner in which the match is made, and the type of computer processing, including the nature of the algorithms, used to make a match.

Human factors also matter. Users need to be aware of how the technology works, its strengths and weaknesses, and how they can ensure the technology functions in a way that complies with all applicable laws and DHS policy. In addition to being operational considerations, these factors also directly affect the civil rights and civil

[1] CRCL has remedial authority under Section 504 of the Rehabilitation Act of 1973, as amended, which states, "No otherwise qualified individual with a disability in the United States . . . shall, solely by reason of her or his disability, be excluded from the participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving Federal financial assistance or under any program or activity conducted by any Executive agency. . . ." 29 U.S.C. § 794.

liberties of those individuals who encounter this DHS technology. In short, the legal and civil rights and civil liberties policy implications of facial recognition technology depend on how the technology is implemented.

CRCL recognizes the potential risks of impermissible bias in facial recognition algorithms, as previously raised by this committee. CRCL supports rigorous testing and evaluation of algorithms used in facial recognition systems to identify and mitigate impermissible bias. CRCL will continue to support the collaborative relationship between NIST, the DHS Science & Technology Directorate, OBIM, and DHS components to that end.

CRCL USES PARTNERSHIPS AND DATA TO LOOK BEYOND THE ALGORITHM

As discussed above, CRCL seeks to ensure civil rights and civil liberties protections are incorporated into Department and component programs—including the policies and practices that guide DHS use of facial recognition technology. Our contribution to DHS working groups is one way we fulfill our mission and identify areas that may require further engagement.

CRCL participates in DHS enterprise-level groups working on biometric and facial recognition issues, including:

- The DHS Executive Steering Committee for Biometric Capabilities, which provides coordination and guidance to all DHS and component-level programs that are developing or providing biometric capabilities in support of DHS mission objectives. The Steering Committee serves as a forum for cross-component collaboration and the sharing of biometric challenges, needs, concepts, best practices, plans and efforts; and
- The Joint Requirements Council's Counter Terrorism and Homeland Threats Portfolio Team, which is made up of component subject-matter experts from the key functional areas within the Department that validate and prioritize requirements and capability gaps, to include those relating to biometrics and screening and vetting functions.

Another way in which we carry out our role in providing proactive advice is through direct engagement with DHS components. For example, CRCL has regularly engaged CBP on the implementation of facial recognition technology in its Biometric Entry-Exit Program. We have viewed live demonstrations of the technology at Dulles International Airport and Hartsfield-Jackson Airport in Atlanta. In addition, we reviewed and commented on internal procedures, as well as proposed regulations. CRCL advised on policy and implementation of appropriate accommodations for individuals wearing religious headwear (e.g., individuals whose headwear may need to be adjusted to take a photograph), for individuals with a sincere religious objection to being photographed, and for individuals who may have a significant injury or disability and for whom taking photographs may present challenges or not be possible. CRCL and the DHS Privacy Office also work cooperatively with the components to address and mitigate issues such as photograph retention and data sharing.

We fully anticipate continuing to provide advice and guidance on DHS's facial recognition programs as they mature and evolve, whether it is through one of the Department's enterprise-level groups or directly with the operational components.

Supporting our advisory role on new or proposed policies or programs, I would also like to highlight the distinctive way CRCL uses the information and allegations we receive as part of our compliance process. In addition to the opening of formal investigations into allegations of civil rights or civil liberties violations, when CRCL does not open an investigation on an allegation, we use the information received to track issues and identify potential patterns of alleged civil rights or civil liberties violations that may require further review. For CBP vetting operations, this data is used to guide CRCL in identifying which policies or programs warrant further investigation to more closely examine potentially serious or systemic issues. Additionally, CRCL shares data with components annually to provide visibility into the civil rights matters CRCL has received, and publishes data on complaints in the Annual and Semi-Annual Reports to Congress.

CRCL'S CONTINUING EFFORTS TO SAFEGUARD CIVIL RIGHTS AND CIVIL LIBERTIES IN DHS'S USE OF EMERGING TECHNOLOGIES

CRCL recognizes that facial recognition technology and the computing that enable it are emerging technologies. They require intensive support from all entities involved—operators, NIST and other researchers, and oversight offices such as CRCL—to ensure that they are compliant with applicable law and policy, including civil rights and civil liberties protections, in all phases of development and deployment. We understand that successful and appropriate facial recognition technology requires on-going oversight and quality assurance, initial validation and regular re-validation, and a close relationship between the users and oversight offices. In this way, it can be developed to work properly and without impermissible bias when it achieves initial operating capability, and then continually through its entire project life cycle. At the same time, we will need to work with the operational components to ensure that policies and practices evolve, to ensure that the human part of the equation—the users—are also focused on the responsible deployment of this technology, working in a manner that consistently prevents impermissible bias in DHS activities.

As these and future projects develop, CRCL will remain engaged with advocates, technologists, experts, and Congress to ensure that civil rights and civil liberties protections are effective and sufficient.

Again, I thank you for the opportunity to appear before you today, and I look forward to answering your questions.

Chairman THOMPSON. Thank you also for your testimony.

I now recognize Dr. Romine to summarize his statement for 5 minutes.

STATEMENT OF CHARLES H. ROMINE, Ph.D., DIRECTOR OF THE INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Mr. ROMINE. Thank you, Chairman Thompson, Ranking Member Rogers, and Members of the committee.

I am Chuck Romine, the director of the Information Technology Laboratory of the National Institute of Standards and Technology, also known as NIST.

Thank you for the opportunity to appear before you today to discuss NIST's role in standards and testing for facial recognition technology.

In the areas of biometrics, NIST has been working with public and private sectors since the 1960's. Biometric technologies provide a means to establish or verify the identity of humans based upon one or more physical or behavioral characteristics.

Face recognition technology compares an individual's facial features to available images for verification or identification purposes. NIST's work improves the accuracy, quality, usability, interoperability, and consistency of identity management systems and ensures that U.S. interests are represented in the international arena.

NIST's research has provided state-of-the-art technology benchmarks and guidance to industry and to U.S. Government agencies that depend upon biometrics recognition technologies.

NIST's face recognition vendor testing program, or FRVT, provides technical guidance and scientific support for analysis and recommendations for utilization of face recognition technologies to various U.S. Government and law enforcement agencies, including the FBI, DHS, CBP, and IARPA.

The NIST FRVT Interagency Report 8280 released in December 2019 quantified the accuracy of face recognition algorithms for demographic groups defined by sex, age, and race or country of birth for both one-to-one and one-to-many identification search algorithms. It found empirical evidence for the existence of demographic differentials in facial recognition algorithms that NIST evaluated.

The report distinguishes between false positive and false negative errors and notes that the impacts of errors are application-dependent.

NIST conducted tests to quantify demographic differences for 189 face recognition algorithms from 99 developers using 4 collections of photographs with 18.27 million images of 8.49 million people.

These images came from operational databases provided by the State Department, the Department of Homeland Security, and the FBI.

I will first address one-to-one verification applications. There, false positive differentials are much larger than those related to false negative and exist across many of the algorithms tested. False positives might present a security concern to the system owner as they may allow access to imposters.

Other findings are that false positives are higher in women than in men and are higher in the elderly and the young compared to middle-aged adults.

Regarding race, we measured higher false positive rates in Asian and African American faces relative to those of Caucasians. There are also higher false positive rates in Native Americans, American Indian, Alaskan Indian, and Pacific Islanders.

These effects apply to most algorithms, including those developed in Europe and the United States. However, a notable exception was for some algorithms developed in Asian countries. There was no such dramatic difference in false positives in one-to-one matching between Asian and Caucasian faces for the algorithms developed in Asia.

While the NIST study did not explore the relationship between cause and effect, one possible connection and an area for research is the relationship between algorithm's performance and the data used to train the algorithm itself.

I will now comment on one-to-many search algorithms. Again, the impact of errors is application-dependent. False positives in one-to-many search are particularly important because the consequences could include false accusations.

For most algorithms, the NIST study measured higher false positive rates in women, African Americans, and particularly in African American women. However, the study found that some one-to-many algorithms gave similar false positive rates across these specific demographics. Some of the most accurate algorithms fell into this group.

This last point underscores one overall message of the report: Different algorithms perform differently.

Indeed, all of our FRVT reports note wide variations in recognition accuracy across algorithms, and an important result from the demographic study is that demographic effects are smaller with more accurate algorithms.

NIST is proud of the positive impact it has had in the last 60 years on the evolution of biometrics capabilities. With NIST's extensive experience and broad expertise both in its laboratories and in successful collaborations with the private sector and other Government agencies, NIST is actively pursuing the standards and measurement research necessary to deploy interoperable, secure, reliable, and usable identity management systems.

Thank you for the opportunity to testify on NIST's activities in facial recognition and identity management, and I would be happy to answer any questions you may have.

[The prepared statement of Dr. Romine follows:]

PREPARED STATEMENT OF CHARLES H. ROMINE

FEBRUARY 6, 2020

INTRODUCTION

Chairman Thompson, Ranking Member Rogers, and Members of the committee, I am Chuck Romine, director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). ITL cultivates trust in information technology and metrology through measurements, standards, and testing. Thank you for the opportunity to appear before you today to discuss NIST's role in standards and testing for facial recognition technology.

BIOMETRIC AND FACIAL RECOGNITION TECHNOLOGY

Home to 5 Nobel Prizes, with programs focused on National priorities such as advanced manufacturing, the digital economy, precision metrology, quantum science, and biosciences, NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In the area of biometrics, NIST has been working with public and private sectors since the 1960's. Biometric technologies provide a means to establish or verify the identity of humans based upon one or more physical or behavioral characteristics. Examples of physical characteristics include face, fingerprint, and iris images. An example of behavioral characteristic is an individual's signature. Used with other authentication technologies, such as passwords, biometric technologies can provide higher degrees of security than other technologies employed alone. For decades, biometric technologies were used primarily in homeland security and law enforcement applications, and they are still a key component of these applications. Over the past several years, the marketplace for biometric solutions has widened significantly and today includes public and private-sector applications world-wide, including physical security, banking, and retail applications. According to one industry estimate, the biometrics technology market size will be worth $59.31 billion by 2025.[1] There has been a considerable rise in development and adoption of facial recognition, detection, and analysis technologies in the past few years.

Face detection technology determines whether the image contains a face. Face analysis technology aims to identify attributes such as gender, age, or emotion from detected faces. Face recognition technology compares an individual's facial features to available images for verification or identification purposes. Verification or "one-to-one" matching confirms a photo matches a different photo of the same person in a database or the photo on a credential, and is commonly used for authentication purposes, such as unlocking a smartphone or checking a passport. Identification or "one-to-many" search determines whether the person in the photo has any match in a database and can be used for identification of a person.

Accuracy of face recognition algorithms is assessed by measuring the two classes of error the software can make: False positives and false negatives. A false positive means that the software wrongly considered photos of 2 different individuals to show the same person, while a false negative means the software failed to match 2 photos that, in fact, do show the same person.

NIST'S ROLE IN BIOMETRIC AND FACIAL RECOGNITION TECHNOLOGY

NIST responds to Government and market requirements for biometric standards, including facial recognition technologies, by collaborating with other Federal agencies, law enforcement, industry, and academic partners to:

- research measurement, evaluation, and interoperability to advance the use of biometric technologies including face, fingerprint, iris, voice, and multi-modal techniques;
- develop common models and metrics for identity management, critical standards, and interoperability of electronic identities;

[1] *https://www.grandviewresearch.com/industry-analysis/biometrics-industry.*

- support the timely development of scientifically valid, fit-for-purpose standards; and
- develop the required conformance testing architectures and testing tools to test implementations of selected standards.

NIST's work improves the accuracy, quality, usability, interoperability, and consistency of identity management systems and ensures that United States interests are represented in the international arena. NIST research has provided state-of-the-art technology benchmarks and guidance to industry and to U.S. Government agencies that depend upon biometrics recognition technologies.

Under the provisions of the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113) and OMB Circular A–119, NIST is tasked with the role of encouraging and coordinating Federal agency use of voluntary consensus standards in lieu of Government-unique standards, and Federal agency participation in the development of relevant standards, as well as promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities. NIST works with other agencies to coordinate standards issues and priorities with the private sector through consensus standards developing organizations such as the International Committee for Information Technology Standards (INCITS), Joint Technical Committee 1 of the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), the Organization for the Advancement of Structured Information Standards (OASIS), IEEE, the Internet Engineering Task Force (IETF), and other standards organizations such as the International Civil Aviation Organization (ICAO), and the International Telecommunication Union's Standardization Sector (ITU–T). NIST leads National and international consensus standards activities in biometrics, such as facial recognition technology, but also in cryptography, electronic credentialing, secure network protocols, software and systems reliability, and security conformance testing—all essential to accelerate the development and deployment of information and communication systems that are interoperable, reliable, secure, and usable.

Since 2010, NIST has organized the biennial International Biometric Performance Testing Conference. This series of conferences accelerates adoption and effectiveness of biometric technologies by providing a forum to discuss and identify fundamental, relevant, and effective performance metrics, and disseminating best practices for performance design, calibration, evaluation, and monitoring.

FACIAL RECOGNITION TESTS AND EVALUATIONS

For more than a decade, NIST biometric evaluations have measured the core algorithmic capability of biometric recognition technologies and reported the accuracy, throughput, reliability, and sensitivity of algorithms with respect to data characteristics, for example, noise or compression, and to subject characteristics, for example, age or gender. NIST biometric evaluations advance the technology by identifying and reporting gaps and limitations of current biometric recognition technologies. NIST evaluations advance measurement science by providing a scientific basis for "what to measure" and "how to measure." NIST evaluations also facilitate development of consensus-based standards by providing quantitative data for development of scientifically sound, fit-for-purpose standards.

NIST conducted the Face Recognition Grand Challenge (2004–2006) and Multiple Biometric Grand Challenge (2008–2010) programs to challenge the facial recognition community to break new ground solving research problems on the biometric frontier.

Since 2000, NIST's Face Recognition Vendor Testing Program (FRVT) has assessed capabilities of facial recognition algorithms for one-to-many identification and one-to-one verification. Participation in FRVT is open to any organization worldwide. There is no charge for participation, and being an on-going activity, participants may submit their algorithms on a continuous basis. The algorithms are submitted to NIST by corporate research and development laboratories and a few universities. As prototypes, these algorithms are not necessarily available as mature integrable products. For all algorithms that NIST evaluates, NIST posts performance results on its FRVT website and identifies the algorithm and the developing organization.

NIST and the FRVT program do not train face recognition algorithms. NIST does not provide training data to the software under test, and the software is prohibited from adapting to any data that is passed to the algorithms during a test.[2]

[2] The process of training a face recognition algorithm (or any machine learning algorithm) involves providing a machine learning algorithm with training data to learn from. The training

Continued

NIST provides technical guidance and scientific support for analysis and recommendations for utilization of facial recognition technologies to various U.S. Government and law enforcement agencies, including the Federal Bureau of Investigation (FBI), Office of Biometric Identity Management (OBIM) at the Department of Homeland Security (DHS), Department of Homeland Security Science and Technology Directorate (DHS S&T), the Department of Homeland Security's U.S. Customs and Border Protection agency (DHS CBP), and the Intelligence Advanced Research Projects Activity (IARPA) at the office of the Director of National Intelligence.

Historically and currently, NIST biometrics research has assisted DHS. For example, NIST's research was used by DHS in its transition to ten prints for the former US–VISIT program. NIST is currently collaborating with DHS OBIM on face image quality standards. Additionally, NIST is working with DHS CBP to analyze performance impacts due to image quality and traveler demographics and provide recommendations regarding match algorithms, optimal thresholds and match gallery creation for its Traveler Verification Service (TVS).

NIST FACE RECOGNITION VENDOR TESTING PROGRAM

NIST's Face Recognition Vendor Testing Program (FRVT) was established in 2000 to provide independent evaluations of both prototype and commercially-available facial recognition algorithms. These evaluations provide the U.S. Government with information to assist in determining where and how facial recognition technology can best be deployed. FRVT results also help identify future research directions for the facial recognition community.

The 2013 FRVT tested facial recognition algorithms submitted by 16 organizations, and showed significant algorithm improvement since NIST's 2010 FRVT test. NIST defined performance by recognition accuracy—how many times the software correctly identified the photo—and the time the algorithms took to match one photo against large photo data sets.

The 2018 FRVT tested 127 facial recognition algorithms from the research laboratories of 39 commercial developers and one university, using 26 million mugshot images of 12 million individuals provided by the FBI. The 2018 FRVT measured the accuracy and speed of one-to-many facial recognition identification algorithms. The evaluation also contrasted mugshot accuracy with that from lower quality images. The findings, reported in NIST Interagency Report 8238,[3] showed that massive gains in accuracy have been achieved since the FRVT in 2013, which far exceed improvements made in the prior period (2010–2013). The accuracy gains observed in the 2018 FVRT study stem from the integration, or complete replacement, of older facial recognition techniques with those based on deep convolutional neural networks. While the industry gains are broad, there remains a wide range of capabilities, with some developers providing much more accurate algorithms than others. Using FBI mugshots, the most accurate algorithms fail only in about ¼ of 1 percent of searches, and these failures are associated with images of injured persons and those with long time lapse since the first photograph. The success of mugshot searches stems from the new generation of facial recognition algorithms, and from the adoption of portrait photography standards first developed at NIST in the late 1990's.

The 2019 FRVT quantified the accuracy of face recognition algorithms for demographic groups defined by sex, age, and race or country of birth, for both one-to-one verification algorithms and one-to-many identification search algorithms. NIST conducted tests to quantify demographic differences for 189 face recognition algorithms from 99 developers, using 4 collections of photographs with 18.27 million images of 8.49 million people. These images came from operational databases provided by the State Department, the Department of Homeland Security, and the FBI. Previous FRVT reports[4] documented the accuracy of these algorithms and showed a wide range in accuracy across algorithms. The more accurate algorithms produce fewer errors and can therefore be anticipated to have smaller demographic differentials.

data shall contain the correct answer, which is known as ground-truth label, or a target. The learning algorithm finds patterns in the training data that map the input data attributes to the target and builds a machine-learning model that captures these patterns. This model can then be used to get predictions on new data for which the target is unknown.

[3] *https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf.*

[4] Part 1: *https://www.nist.gov/system/files/documents/2019/11/20/frvt__report__2019__11__19__0.pdf* and Part 2: *https://www.nist.gov/system/files/documents/2019/09/11/nistir__8271__20190911.pdf.*

NIST Interagency Report 8280,[5] released on December 19, 2019, quantifies the effect of age, race, and sex on face recognition performance. It found empirical evidence for the existence of demographic differentials in face recognition algorithms that NIST evaluated. The report distinguishes between false positive and false negative errors, and notes that the impacts of errors are application dependent.

I will first address one-to-one verification applications. There, false positive differentials are much larger than for false negatives and exist across many, but not all, algorithms tested. Across demographics, false positives rates often vary by factors of 10 to beyond 100 times. False negatives tend to be more algorithm-specific, and often vary by factors below 3. False positives might present a security concern to the system owner, as they may allow access to impostors. False positives may also present privacy and civil rights and civil liberties concerns such as when matches result in additional questioning, surveillance, errors in benefit adjudication, or loss of liberty. False positives are higher in women than in men and are higher in the elderly and the young compared to middle-aged adults. Regarding race, we measured higher false positive rates in Asian and African American faces relative to those of Caucasians. There are also higher false positive rates in Native American, American Indian, Alaskan Indian, and Pacific Islanders. These effects apply to most algorithms, including those developed in Europe and the United States. However, a notable exception was for some algorithms developed in Asian countries. There was no such dramatic difference in false positives in one-to-one matching between Asian and Caucasian faces for algorithms developed in Asia. While the NIST study did not explore the relationship between cause and effect, one possible connection, and area for research, is the relationship between an algorithm's performance and the data used to train the algorithm itself.

I will now comment on one-to-many search algorithms. Again, the impact of errors is application-dependent. False positives in one-to-many search are particularly important because the consequences could include false accusations. For most algorithms, the NIST study measured higher false positives rates in women, African Americans, and particularly in African American women. However, the study found that some one-to-many algorithms gave similar false positive rates across these specific demographics. Some of the most accurate algorithms fell into this group. This last point underscores one overall message of the report: Different algorithms perform differently. Indeed all of our FRVT reports note wide variations in recognition accuracy across algorithms, and an important result from the demographics study is that demographic effects are smaller with more accurate algorithms.

A general takeaway from these studies is that, there is significant variance between the performance facial recognition algorithms, that is, some produce significantly fewer errors than others. Consequently, users, policy makers, and the public should not think of facial recognition as either always accurate or always error prone.

NIST FACE IN VIDEO EVALUATION PROGRAM

The Face in Video Evaluation Program (FIVE) assessed the capability of facial recognition algorithms to correctly identify or ignore persons appearing in video sequences. The outcomes of FIVE are documented in NIST Interagency report 8173,[6] which enumerates accuracy and speed of facial recognition algorithms applied to the identification of persons appearing in video sequences drawn from 6 different video datasets. NIST completed this program in 2017.

HUMAN FACTORS: FACIAL FORENSIC EXAMINERS

NIST is researching how to measure the accuracy of forensic examiners matching identity across different photographs. The study measures face identification accuracy for an international group of professional forensic facial examiners working under circumstances approximating real-world casework. The findings, published in the proceedings of the National Academy of Sciences,[7] showed that examiners and other human face "specialists," including forensically-trained facial reviewers and untrained super-recognizers, were more accurate than the control groups on a challenging test of face identification. It also presented data comparing state-of-the-art facial recognition algorithms with the best human face identifiers. The best machine performed in the range of the best-performing humans, who were professional facial

[5] *https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.*

[6] *https://www.nist.gov/publications/face-video-evaluation-five-face-recognition-non-cooperative-subjects.*

[7] *https://www.pnas.org/content/115/24/6171.*

examiners. However, optimal face identification was achieved only when humans and machines collaborated.

VOLUNTARY CONSENSUS STANDARDS

When properly conducted, standards development can increase productivity and efficiency in Government and industry, expand innovation and competition, broaden opportunities for international trade, conserve resources, provide consumer benefit and choice, improve the environment, and promote health and safety.

In the United States, most standards development organizations are industry-led private-sector organizations. Many voluntary consensus standards from those standard development organizations are appropriate or adaptable for the Government's purposes. OMB Circular A–119 directs the use of such standards by U.S. Government agencies, whenever practicable and appropriate, to achieve the following goals:

- eliminating the cost to the Federal Government of developing its own standards and decreasing the cost of goods procured and the burden of complying with agency regulation;
- providing incentives and opportunities to establish standards that serve National needs, encouraging long-term growth for U.S. enterprises and promoting efficiency, economic competition, and trade; and
- furthering the reliance upon private-sector expertise to supply the Federal Government with cost-efficient goods and services.

EXAMPLES OF NIST CONSENSUS STANDARDS DEVELOPMENT ACTIVITIES

ANSI/NIST–ITL.—The ANSI/NIST–ITL standard for biometric information is used in 160 countries to ensure biometric data exchange across jurisdictional line and between dissimilar systems. One of the important effects of NIST work on this standard is that it allows accurate and interoperable exchange of biometrics information by law enforcement globally and enables them to identify criminals and terrorists. NIST's own Information Technology Laboratory is an American National Standards Institute (ANSI)-accredited standard development organization. Under accreditation by ANSI, the private-sector U.S. standards federation, NIST continues to develop consensus biometric data interchange standards. Starting in 1986, NIST has developed and approved a succession of data format standards for the interchange of biometric data. The current version of this standard is ANSI/NIST–ITL 1: 2015, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information.[8] This standard continues to evolve to support Government applications including law enforcement, homeland security, as well as other identity management applications. Virtually all law enforcement biometric collections world-wide use the ANSI/NIST–ITL standard. NIST biometric technology evaluations in fingerprint, face, and iris have provided the Government with timely analysis of market capabilities to guide biometric technology procurements and deployments.

ISO/IEC JOINT TECHNICAL COMMITTEE 1, SUBCOMMITTEE 37 (JTC1/SC37)—BIOMETRICS

From the inception of the ISO Subcommittee on Biometrics in 2002, NIST has led and provided technical expertise to develop international biometric standards in this subcommittee. Standards developed by the Subcommittee on Biometrics have received wide-spread international and National market acceptance. Large international organizations, such as the ICAO for Machine-Readable Travel Documents and the International Labour Office (ILO) of the United Nations for the verification and identification of seafarers, specify in their requirements the use of some of the international biometric standards developed by this subcommittee.

Since 2006, JTC1/SC37 has published a series of standards on biometric performance testing and reporting, many of which are based on NIST technical contributions. These documents provide guidance on the principles and framework, testing methodologies, modality-specific testing, interoperability performance testing, access control scenarios, and testing of on-card comparison algorithms for biometric performance testing and reporting. NIST contributes toward the development of these documents and follows their guidance and metrics in its evaluations, such as the FRVT.

CONCLUSION

NIST is proud of the positive impact it has had in the last 60 years on the evolution of biometrics capabilities. With NIST's extensive experience and broad exper-

[8] *https://www.nist.gov/publications/data-format-interchange-fingerprint-facial-other-biometric-information-ansinist-itl-1-1.*

tise, both in its laboratories and in successful collaborations with the private sector and other Government agencies, NIST is actively pursuing the standards and measurement research necessary to deploy interoperable, secure, reliable, and usable identity management systems.

Thank you for the opportunity to testify on NIST's activities in facial recognition and identity management. I would be happy to answer any questions that you may have.

Chairman THOMPSON. Thank you very much.

I thank all of the witnesses for their testimony.

I remind each Member that he or she will have 5 minutes to question the panel.

I will now recognize myself for questions.

Dr. Romine, we will start off with you. Part of your NIST report was like next generation technology, as I understand, that CBP will use or did you review existing technology?

Mr. ROMINE. We are not certain of that. We certainly intend to continue our investigations. The existence of the specific algorithms that we test, those algorithms are submitted to us by the vendors. We have no independent way to correlate whether those are the identical algorithms that are being used in the field.

Chairman THOMPSON. So part of what you said is how the technology is deployed depends on the application of the technology. Explain that a little more to the committee.

Mr. ROMINE. Certainly. Our approach is that the significant thing to be cognizant of is the risk associated with the deployment, and the studies that we do help to inform policy makers, such as Members of Congress, as well as operators of these technologies, about how to quantify those risks at least for the algorithms themselves.

The deployed systems have other characteristics associated with them that we do not test. We test only the algorithms currently.

The second point is that that risk that comes from the error rates associated with the algorithms is part of a much larger risk management that the operators have to undertake.

For example, access to critical infrastructures and access control systems to critical infrastructures is different than access to a phone that you might have. The risks are different in those cases.

Chairman THOMPSON. Thank you.

Mr. Wagner, can you share with the committee the extent that CBP goes to to protect the information collected in this process?

Mr. WAGNER. Sure. So the photographs that are taken by one of our stakeholders' cameras, they are encrypted. They are transmitted securely to the CBP cloud infrastructure where the gallery is positioned.

Chairman THOMPSON. Right.

Mr. WAGNER. The pictures are templatized, which means they are turned into some type of mathematical structure that cannot be reverse-engineered, and they are matched up with the templatized photos that we have pre-staged in the gallery, and then just a response goes back, yes or no, with a unique identifier.

Chairman THOMPSON. Thank you.

So the comment that 2 to 3 percent of people who are misidentified, what is CBP doing to try to get that to zero?

Mr. WAGNER. Right. So it is not that they are misidentified. It just means we did not match them to a picture in the gallery that we did have of them. So we should have matched them.

You are right. That should be at zero, and that is where we look at the operational variables, the camera, the picture quality, the human behaviors when the photo was taken, the lighting, those different types, and then the age of the photo.

Then what we have seen in the NIST report, your gallery size impacts your match rate. I think NIST tested galleries up to 12 million size. We are comparing against a few thousand here at most.

Then the numbers of photos that we have of the particular individual can impact which one we match against and then some of your match rates, and then the age of the photo. So if you had your passport taken at age 20 and you are now 29 and your face has changed in the dimensions, we are going to struggle to match against that, which is then compounded by poor lighting conditions or the person moving when the photo is taken or a poorer-quality photo.

Chairman THOMPSON. Well, Mr. Mina, listening to what you just heard, have you all dealt with any complaints from citizens about this technology?

Mr. MINA. Mr. Chairman, we have received one complaint that referenced this facial recognition technology. However, we have not seen a trend, and that is when we would actually, in fact, open an investigation in this matter.

We are working, as I mentioned, on the policy side of the house advising CBP directly.

The other way in which we also hear from the community, as you may know, is through our Community Engagement Roundtables around the country, and we have heard concerns in those forums about facial recognition technology, and those are concerns that we are using to inform our advice.

Chairman THOMPSON. So can you provide the committee with where you have held those forums around the country?

Mr. MINA. Yes, absolutely.

We do roundtables in about 18 cities, and not to say that these concerns have been raised in every single location, but certainly in some.

Then, again, we will continue to have those discussions with CBP and with S&T in the future at future roundtables.

Chairman THOMPSON. Thank you.

Last, Mr. Wagner, I am not sure you have information on this, but last month Iranian and Lebanese nationals and individuals who travel to Iran and Lebanon, most of whom were U.S. citizens or green card holders, were targeted, detained, and subjected to prolonged questioning of up to 12 hours at the Blaine area port of entry. I understand an internal CBP memo indicates people were also questioned based on their religion, which is completely unacceptable.

I understand CBP has admitted to enormous mistakes in this incident. If you know, how did this situation happen?

What is CBP doing to ensure that it never happens again?

Mr. WAGNER. So there was no National directive or guidance that went out other than because of the things taking place in Iran, the concerns about retaliation, we put our field managers on alert to be more vigilant about current events that are happening and work with your State, local, and Federal counterparts and, you know, really just be vigilant.

There was some more prescriptive guidance that went out at the local level in Blaine, Washington, which we are reviewing right now because there are a lot of concerning things, I think, that we saw in the interpretation of that guidance and the management oversight as that weekend was unfolding and people were being referred in for additional inspections and questioning, and there are some concerning points about the management engagement or lack thereof of what transpired.

So there is an internal investigation that CBP is conducting. Civil Rights and Civil Liberties is conducting an investigation, and when we get the results of that, we will then proceed, you know, accordingly, depending on what those results say.

Chairman THOMPSON. Mr. Mina, were you aware of that?

Mr. MINA. Yes, and as Mr. Wagner said, we do have an open investigation in this matter.

Chairman THOMPSON. OK. Thank you.

Ranking Member, are you ready?

Mr. ROGERS. I am ready. Thank you.

Chairman THOMPSON. I yield to the Ranking Member for an opening statement.

Mr. ROGERS. I am sorry for being late. We just got back from the National Prayer Breakfast.

Thank you, Mr. Chairman.

After the tragic events of September 11, Congress recognized that biometric systems are essential to our homeland security. Following the recommendation of the 9/11 Commission, Congress charged DHS with the creation of an automated, biometric entry and exit system.

Customs and Border Protection and the Transportation and Security Administration have already demonstrated the capability of biometrics to improve security, facilitate travel, and better enforced existing immigration law.

Government and the private sector have made enormous strides in the accuracy, speed, and deployment of biometric systems. Biometric technologies of all types have seen improvements.

These advances in facial recognition algorithms, in particular, are transformational. The National Institute of Standards and Technology is the leader in testing and evaluation for biometric technologies.

Dr. Romine and his team have done incredible work to help Congress, DHS, and industry understands the capability of currently available algorithms, but I am concerned that some of my colleagues have already jumped to the misleading conclusion that NIST reports on facial recognition.

Just hours after NIST released the 1,200 pages of technical data, the Majority tweeted that this report shows facial recognition is even more unreliable and racially biased than we feared. If the Majority had taken the time to read the full report before tweeting, they would have found that the real headline, NIST determined that facial recognition algorithms being adopted by DHS has no statistically detectable race or gender bias.

In other words, NIST could find no statistical evidence that facial recognition algorithms that DNS is adopting contains racial bias.

I hope my colleagues will listen to Dr. Romine as he explains how the NIST report proves that race or gender bias is statistically undetectable in the most accurate algorithms.

The reality is that facial recognition technologies can improve existing processes by reducing human error. These technologies are tools that cannot and will not replace the final judgment of CBP or TSA officers.

Concerns regarding privacy and civil rights are well-intentioned, but these concerns can be fully addressed in how biometric systems are implemented by DHS.

I look forward to hearing the steps that CRCL is taking to coordinate with CBP and to protect privacy and civil rights of Americans.

But as I have said before, halting all Government biometric programs is not a solution. Doing so ignores the critical facts that the technology that DHS uses is not racially biased. It does not violate the civil rights of Americans. It is accurate. Most importantly, it does protect the homeland.

I appreciate the Chairman calling the hearing today. It is important for Congress to further educate itself on this issue. I look forward to getting the facts, and I yield back, Mr. Chairman.

[The statement of Ranking Member Rogers follows:]

STATEMENT OF RANKING MEMBER MIKE ROGERS

FEBRUARY 6, 2020

After the tragic events of September 11, Congress recognized that biometric systems are essential to our homeland security.

Following the recommendation of the 9/11 Commission, Congress charged DHS with the creation of an automated biometric entry and exit system.

Customs and Border Protection and the Transportation Security Administration have already demonstrated the capability of biometrics to improve security, facilitate travel, and better enforce existing immigration laws.

Government and the private sector have made enormous strides in the accuracy, speed, and deployment of biometrics systems.

Biometric technologies of all types have seen improvements.

The advances in facial recognition algorithms in particular are transformational.

The National Institute of Standards and Technology is the leader in testing and evaluation for biometric technologies.

Dr. Romine and his team have done incredible work to help Congress, DHS, and industry understand the capability of currently-available algorithms.

But I'm concerned that some of my colleagues have already jumped to misleading conclusions regarding the NIST report on facial recognition.

Just hours after NIST released over 1,200 pages of technical data, the Majority tweeted “This report shows facial recognition is even more unreliable and racially biased than we feared . . . [”.

If the Majority had taken the time to read the full report before tweeting, they would have found the real headline: NIST determined that the facial recognition algorithm being adopted by DHS had no statistically detectable race or gender bias.

In other words, NIST could find NO statistical evidence that the facial recognition algorithm DHS is adopting contains racial bias.

NIST found measurable and significant errors and bias in OTHER facial recognition algorithms, but NOT in the algorithm used by DHS.

I hope that my colleagues will listen when Dr. Romine explains how the NIST report proves that race or gender bias is statistically undetectable in the most accurate algorithms.

The reality is that facial recognition technologies can improve existing processes by reducing human error.

These technologies are tools that cannot and will not replace the final judgment of CBP or TSA officers.

Concerns regarding privacy and civil rights are well-intentioned.

But these concerns can be fully addressed in how biometric systems are implemented by DHS.

I look forward to hearing the steps CRCL is taking to coordinate with CBP and protect the privacy and civil rights of Americans.

But as I have said before, halting all Government biometric programs is not the solution.

Doing so ignores these critical facts: The technology DHS uses is NOT racially biased; It does NOT violate the civil rights of Americans; It IS accurate; and most importantly, it DOES protect the homeland.

I appreciate the Chairman calling this hearing today. It's important for Congress to further educate itself on this issue. I look forward to getting the facts on the record.

Chairman THOMPSON. Thank you very much.

I wish you had heard the testimony because there was some testimony we heard to the contrary.

Mr. ROGERS. I look forward to probing them on that.

Chairman THOMPSON. All right. Well, I recognize the gentleman for his questions.

Mr. ROGERS. My statement is wrong, to get to the Chairman's point. Anybody can jump at it.

Mr. WAGNER. I would never tell Congress they are wrong.

Mr. ROGERS. You are one of the few people who will not do that.

[Laughter.]

Mr. ROGERS. Literally, I mean, my understanding is there is no statistical evidence that there is racial bias. Is that an inaccurate statement?

Mr. ROMINE. Thank you for the question.

In the highest-performing algorithms for one-to-many matches, the highest-performing algorithms we saw undetectable bias. The demographic differentials that we were measuring we say are undetectable in the report.

Mr. ROGERS. So what do you mean by undetectable?

Mr. ROMINE. What I mean by that is that in the testing that we undertook, there was no way to determine—let me back up and say the idea of having absolutely zero false positives is a big challenge.

Mr. ROGERS. Did you test the NEC–3 algorithm being used by DHS?

Mr. ROMINE. We tested algorithms from NEC. We have no independent way to verify that that is the specific algorithm that is being used by CBP. That would be something that CBP and NEC would have to attest to.

From our perspective, the vendor provides us algorithms. They are black boxes that we test just the performance of the algorithm that is submitted to us by the vendor.

Mr. ROGERS. Mr. Wagner, is CBP currently working to implement NEC–3 algorithms?

Mr. WAGNER. Any what? I am sorry.

Mr. ROGERS. NEC–3 algorithms.

Mr. WAGNER. Yes, we are using an earlier version of NEC right now, and I believe we are testing NEC–3, which is the version that was tested, and the plan is to use it next month in March to switch or to upgrade basically to that one.

Mr. ROGERS. OK. Dr. Romine, who can participate in the facial recognition vendor test? Is it accurate to say that some algorithms are far less accurate and sophisticated than others?

Mr. ROMINE. Yes, sir, that is correct. Anyone around the globe can participate. We have participants from industries, biometrics industries around the country, but also from universities and some experimental systems as well.

Mr. ROGERS. Great. That is all I have, Mr. Chairman. Thank you.

Chairman THOMPSON. Thank you very much.

Mr. Wagner, let's get clear. The C–3, you do not have it operational anywhere in the country, right? You are testing it.

That technology goes into being, you said, next month?

Mr. WAGNER. The NEC–3 algorithm we are planning to implement next month. The earlier version of it is operational now.

Chairman THOMPSON. But the one we are talking about is not?

Mr. WAGNER. Correct.

Chairman THOMPSON. Dr. Romine, let's be clear. You mentioned that African Americans and Asians get misidentified.

Mr. ROMINE. In the highest-performing algorithms we do not see that to a statistical level of significance, for one-to-many algorithms, the identification algorithms.

For the verification algorithms, we do see or the one-to-one algorithms we do see evidence of demographic effects for African Americans, for Asians, and others.

Chairman THOMPSON. Thank you.

The Chair recognizes Ms. Slotkin for 5 minutes.

Ms. SLOTKIN. Thank you.

Thank you for clarifying that because it was hard to understand from your testimony.

So just to be clear, Dr.—I am sorry. Can you pronounce your name? I want to pronounce it right.

Mr. ROMINE. Romine.

Ms. SLOTKIN. Romine. Sorry. Apologies.

Mr. ROMINE. That is quite all right.

Ms. SLOTKIN. So in a certain segment of these algorithms, there is some evidence that they have higher rates of mistakes for African Americans and Asian Americans; is that correct?

Mr. ROMINE. It is correct that most of the algorithms in the one-to-many that are submitted do exhibit those differentials. The highest performing ones in the one-to-many do not.

Ms. SLOTKIN. OK. So some do and some do not. I am just trying to clarify.

Thank you all for being here. I am from Michigan. So we have a long history of needing our CBP officers to protect us at the Detroit airport and all of our bridges and crossings. So can you help me understand?

Is this technology, Mr. Wagner, being used in any way at our bridge crossings in the Northern Border?

Mr. WAGNER. No, not at the bridge crossings.

Ms. SLOTKIN. OK. But at the airport.

Mr. WAGNER. At the airport.

Ms. SLOTKIN. I know at the airport.

So while I recognize it seems to be a small number of times or of these programs where they have detected more problems with particularly African American women I think were mentioned and Asian Americans, walk me through the process where it would be you are an average citizen. You are from my district. You are an African American woman.

Let's say we employ this technology and it shows a positive, right, a link. Just walk me through that process and how you would deal with that at the actual border for that actual citizen.

Mr. WAGNER. You would then just show your passport, which is what you do today, and a person would manually review it if you did not match.

Ms. SLOTKIN. If they showed the passport but the technology still showed a match, what does that officer do in that situation, if the machine is saying one thing and the passport is saying another?

Mr. WAGNER. We would go on the basis of the document we are presenting and which photograph we have identified you with or which identity we have identified you with.

Ms. SLOTKIN. OK. Then that person would cross the border and go on with their—I am just asking.

Mr. WAGNER. Yes.

Ms. SLOTKIN. For the average person to understand how this is being implemented.

Mr. WAGNER. What we are matching people against, U.S. citizens, is that passport photo. We have an electronic copy of that passport database. So——

Chairman THOMPSON. Excuse me just a minute.

Staff, you all are being most disrespectful to the hearing.

Please.

Mr. WAGNER. So when you are flying into the country, you preassemble a gallery of those photographs, and that is what we match you against. So on the officer's screen, they will see the photograph which should be also what is printed on your passport, which also should be on that electronic chip in your passport.

We will look at you and make sure you are all that same person. If it does not match against that, then we will have to figure out why.

Ms. SLOTKIN. When you figure out why, is that individual allowed to progress?

You know, we got to Windsor to like see a concert, and we go to Canada quite often in Michigan.

Mr. WAGNER. Right. It could be as simple as just looking at your passport document and saying, "OK. That's you."

Ms. SLOTKIN. OK.

Mr. WAGNER. Then we will figure out later what happened.

Ms. SLOTKIN. Then what happens with that data, right?

So let's say a woman has gone to her concert in Canada. What happens to her data where it is flagged that she is falsely flagged that she is matched against someone who has done something wrong?

What happens in the Department to that information?

Mr. WAGNER. If you are a U.S. citizen, the new photograph we take is discarded after 12 hours. There is no need for us to keep the new photograph.

There is a record of the transaction that you crossed the border. If there is some type of error in that, then our analysts would look at it and correct it basically.

If you have matched, which happens very often in a biographical sense, your name, date of birth, to the wrong person even though your biographic match is identical to someone else, that is where we can also use the facial recognition to help us distinguish between the people with the common names.

We can put notes in the system then to advise the officers to suppress that information from even appearing when we query your passport the next time.

Ms. SLOTKIN. Tell me how this technology where you have been implementing it at different airports and different land borders, I understand, in the South. Tell me: What are the results?

How many people have you identified in a positive way that needed to be identified?

Tell me some statistics to help me to demonstrate the value of these programs.

Mr. WAGNER. Sure. It is 43.7 million people we have run through it to date at all the different locations, inbound, outbound, cruise ships, land border pedestrians. We have caught 252 imposters, people with legitimate travel documents belonging to someone else. I think 75 of those were U.S. travel documents.

Remember for U.S. travel documents the only biometric we have is that digitized photo that the State Department has put on the electronic chip. There is no fingerprint record. There is no fingerprint requirement to get a U.S. passport.

I am not advocating for one, but there is not one there. So the only biometric we have on a U.S. travel document is that digitized photograph, and that is a worldwide standard.

That chip is allowed to be opened by any country participating in that ICAO scheme that can access the chip and pull off the digital photograph and then do some type of comparison to that.

Ms. SLOTKIN. So in my remaining time, so tens of millions of people that you have used that have gone through this technology, just tell me a little bit more about your stats. How many positive stories? How many negative hits?

Mr. WAGNER. So our match rate is about 97 to 98 percent. That 2 to 3 percent generally means we could not find that person in that preassembled gallery, meaning we did not match against anything. We did not match against the wrong person. We just did not find a match of people traveling.

It could be various environmental or operational reasons for why that happened.

Ms. SLOTKIN. How many are false positives?

Mr. WAGNER. I am not aware of any.

Ms. SLOTKIN. OK.

Mr. WAGNER. But there may be a small handful. I am just not aware of any, but as we built this and tested it, we are just not seeing that.

Ms. SLOTKIN. I think my time has expired. Thank you, gentlemen.

Chairman THOMPSON. Thank you.

The Chair recognizes the gentleman from Texas, Mr. McCaul.

Mr. MCCAUL. Thank you, Mr. Chairman.

You know, the 9/11 Commission recommended the use of biometrics for those entering and leaving the United States, and I believe that technology is our friend in stopping terrorists and bad actors from entering this country.

We have seen it time and time again, and my first question is my understanding is the entry/exit program, American citizens can opt out of that program. Is that correct?

Mr. WAGNER. Yes, that is correct.

Mr. MCCAUL. So there is no requirement that all Americans have to be subjected to this.

Mr. WAGNER. No, but people have to like establish their identity.

Mr. MCCAUL. Yes.

Mr. WAGNER. Once we determine either through manual review of the passport or by using the technology, they are a U.S. citizen and they are excluded from the biometric tracking requirement.

Mr. MCCAUL. Right.

Mr. WAGNER. But they can opt out of having their picture taken to make that determination.

Mr. MCCAUL. It is just like we use with global entry. Most of my constituents love global entry. You know, I got the CLEAR Program, as did Mr. Katko, associated with TSA so you could put your fingerprints down and get to the head of the TSA PreCheck line.

These are the technologies. I think it made it easier for the traveling public, but also the great thing is it does not lie. Biometrics, it is you, and it is hard to fake that.

The last Congress we passed out of the committee my bill, the Biometric Identification Transnational Migration Alert Program, otherwise known as BITMAP. Now, I know this is an ICE program, not CBP, but it passed overwhelmingly in a bipartisan way on the floor, 272 to 119.

It reauthorizes successful programs started under the Obama administration that Secretary Jeh Johnson and I talked a great deal about.

How can we use BITMAP to identify when these people were coming into our hemisphere?

They may change their names multiple times along the route to get to the United States, yet their facial recognition, their biometrics do not. Their names do, but not their biometrics.

This has been, in my judgment, a very successful program in keeping terrorists, human traffickers, and bad actors out of this country.

In fact, this program has enrolled over 155,000 encounters of persons of interest and 460 known and suspected terrorists, including arresting violent criminals and rapists involved in transnational criminal organizations.

So, again, Mr. Wagner, can you comment on why that program is so valuable to the security of the United States and the American people?

Mr. WAGNER. Sure. It is critically important because, as you mentioned, people do change their biographic details, and you know, most of our watch list searches are biographically-based.

But if we can identify people, especially people traveling via air, that we have National security concerns about and they are entering our hemisphere, if they are entering in Central or South America, we can work with our partners down there and establish on a biometric basis who that person is so that no matter what identity they show up in later, if they show up on the U.S.-Mexico border, we can run the biometric confirmation to see, well, who were they when they first flew into the hemisphere. It is critically important.

Mr. MCCAUL. The travel documents can change and passports are stolen and manufactured.

Mr. WAGNER. Absolutely.

Mr. MCCAUL. That is not accurate, but the biometrics do not lie.

Mr. WAGNER. Correct. People change documents, steal documents, borrow documents, purchase documents.

It is harder to alter them now, but the ability to get a legitimate document that looks like you, and if you can pass by the visual inspection of somebody glancing at the little 2×2 photograph on it, yes, yes, and that is where the risk is.

Mr. MCCAUL. It is unfortunate the Senate in its usual wisdom did not pass this bill. They stole a lot of legislation the Chairman and I in a bipartisan way passed last Congress, and that is unfortunate. I would hope we could pass this bill again this Congress.

I do think we have to look at civil liberties and privacy as well, but I do think entry/exit is opt-out. It applies primarily to Americans who would want to opt in and foreign nationals, and BITMAP applies really almost really to foreign nationals themselves.

So I want to thank the witnesses for your testimony.

Mr. Chairman, thanks for having this hearing. I yield back.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the gentlelady from New York, Ms. Clarke.

Ms. CLARKE. Thank you very much, Mr. Chairman. I thank our Ranking Member. I thank our expert witnesses who testified before us today.

But it is time that we face the fact. Unregulated, facial recognition is just not an option. We can debate and disagree about the exact situations where we should permit the use of facial recognition, but we should all agree that there is no situation where facial recognition should be used without safeguards against bias and protections for privacy.

Right now in terms of regulation, facial recognition is still in the Wild West. Meanwhile facial recognition technologies are routinely misidentifying women and people of color.

Although there are some promising applications for facial recognition, these benefits do not outweigh the risk of automating discrimination.

We have seen what happens when technology is widely deployed before Congress can impose meaningful safeguards. So let us all look before we leap.

Mr. Wagner, some of our staff have observed issues with facial recognition technology screening at airports. For example, we have seen passengers, and particularly darker-skinned passengers it seems, not able to be matched due to poor lighting or other factors.

Does CBP track how often its systems failed to capture photos of sufficient quality for matching?

Mr. WAGNER. We track the number of—well, we do not own all of the cameras. So it is difficult for us to track what an airline does or how many pictures they might be taking before they submit one to us for matching. Because in the departure environment, the airports or the airlines are the ones that own them.

So we are tracking how many pictures we receive and what our match rates against them are.

Ms. CLARKE. Yes, I was just wondering about the quality because if the photo quality is not good enough, the accuracy of the matching algorithm is irrelevant.

Mr. WAGNER. Absolutely. So we set a minimum standard. The picture has to be of this quality before it even——

Ms. CLARKE. But do you track the numbers of photos that do not meet your standard?

You said you have all of these other partners that are taking photos.

Mr. WAGNER. Right.

Ms. CLARKE. If you are using their material, then now you are dealing with something that has become irrelevant if you do not know what subset of those do not meet your quality control, right?

Mr. WAGNER. Well, we know the pictures that they transmit to us, whether or not they meet——

Ms. CLARKE. Right. But have you——

Mr. WAGNER. But we do not know how many attempts they made.

Ms. CLARKE. Absolutely, and you do not know the quality. You do not know how much of that, what percentage of that does not meet your standard.

Mr. WAGNER. Well, we look at the number of passengers on——

Ms. CLARKE. Do you know the percentage that does not meet your standard?

Mr. WAGNER. Not offhand, no.

Ms. CLARKE. OK. How does CBP plan to address these issues to ensure it can capture high-quality images of travelers for successful facial recognition screening?

Mr. WAGNER. That is the partnership with NIST where we look at. We have a high-performing algorithm. Now we look at the operational variables to make that even more high-performing.

Ms. CLARKE. So what I would say to you is that then until you have met that standard, you are not doing the public a service.

Mr. WAGNER. What standard is that?

Ms. CLARKE. Of quality control.

Mr. WAGNER. We are developing that standard.

Ms. CLARKE. Right. It is not developed, right? You're developing.

Mr. WAGNER. Not necessarily, no. I mean, what we are seeing, if we are matching it at 97 to 98 percent rate, we are getting——

Ms. CLARKE. Let me go on to another question.

When you are in that 3 percent, it does not matter about the other——

Mr. WAGNER. We are not seeing demographic-based, you know, rates in that 3 percent, and that is when we partnered with NIST to come in and help us understand that better to be sure that that is the case.

Ms. CLARKE. Very well. Very well.

I understand that since our last hearing CBP completed operational testing of the biometric entry/exit systems at airports. The results indicated that the system accurately matched images when captured, but the rate of successfully capturing an image was significantly lower than expected, 80 percent compared to 97 percent.

Most of these issues were attributed to airlines reverting to manually processing passengers to speed the boarding process. Are you aware of these findings?

Mr. WAGNER. Yes, and that is as we were developing the operational variables to look at, No. 1, does it even work, right? Can we make it work?

Now we look at and we work with the airlines to not shut down their boarding. What is the ease of the application of the traveler engaging with that?

Ms. CLARKE. So quickly, what steps is CBP taking to work with airlines to increase image capture rates?

Mr. WAGNER. So one is publishing the regulation, which would then put the requirement onto the foreign national who has to comply with the biometric exit Congressional mandate.

Then we can work with the carriers to increase the rate at which people——

Ms. CLARKE. Can you provide our committee with those steps? That would be helpful.

Mr. WAGNER. Sure. Absolutely.

Ms. CLARKE. Let me ask just quickly because I have run out of time.

Mr. Mina, you spoke in your testimony about impermissible bias, and I was just wondering since you used that terminology, is there something called permissible bias?

Mr. MINA. I think if I understand your question correctly, the reason why we used that term "impermissible bias" is because, as Mr. Wagner has talked about and Mr. Romine has talked about, there are lots of reasons why there may be failure to cause a match, like, you know, for example, lighting, environment.

But our office is really focused on an error that is created based on a protected characteristic, like race or sex or age. When I make that reference to impermissible bias that is what I am referring to.

Ms. CLARKE. So there is no bias that is permissible. In other words, if there is a quirk of some sort and you find it to be so inconsequential that it becomes part of your standard, that becomes permissible bias?

I am just trying to understand what you mean by impermissible bias.

Mr. MINA. Again, I think what I am focusing on is what is actually prohibited by law that our office would look at, which is really based on those protected characteristics.

Now, of course, you know, obviously CBP and folks across the Department are trying to eliminate any bias if they find any reason. However, in terms of what we do as a policy office, we are really focused on the potential for bias in those protected areas.

Ms. CLARKE. Very well. I yield back. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you.

The Chair recognizes the gentleman from New York, Mr. Katko.

Mr. KATKO. Thank you, Mr. Chairman, and I appreciate you having this hearing. This is very important.

I commend all of my colleagues for their probing questions because it is important, but I will make this general observation based on my time as a prosecutor.

When I was first a prosecutor, DNA evidence was this weird science thing that no one really knew about, and as we went on and as it got refined and as it got better, it became a very potent tool not just for law enforcement, but to exonerate people who were wrongly accused of crimes.

I see the biometric technology filling a similar role. It is going to help law enforcement. It is also going to do a dramatically good thing to prevent misidentification of criminal conduct, and I am heartened for that.

So one of the things I am heartened most about that I heard today was from Dr. Romine that the highest-performing algorithms have no statistical anomalies, if I understand that correctly.

So that means that at some point those algorithms will get to the front lines, and I encourage you to get them to the front lines quickly.

I encourage Mr. Mina never to let your guard down and always follow any problems with these systems and make it better because in the end, we are all going to benefit.

I trust my colleagues will ask other probing questions. So I have to ask something of Mr. Wagner that occurred yesterday that is very important to my constituents, in general, but to New York State, in particular.

A letter was sent February 5, 2020, which was yesterday, to New York State saying why Homeland Security can no longer have New York driver's licenses as part of the formula for the Trusted Traveler Program, and that is because New York State under the Green Light Law, which it passed, forbids access by CBP and ICE to the New York driver databases.

So could you briefly summarize for us, and I will ask that this letter be incorporated into the record, Mr. Chairman, first of all.

I ask that the letter be incorporated into the record.

Chairman THOMPSON. Without objection.

[The information referred to follows:]

LETTER FROM CHAD F. WOLF, ACTING SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

February 5, 2020.

Mark J.F. Schroeder,
Acting Commissioner, New York State Department of Motor Vehicles, 6 Empire State Plaza, Albany, NY 12228, mark.schroeder@dmv.ny.gov.

Theresa L. Egan,
Executive Deputy Commissioner, New York State Department of Motor Vehicles, 6 Empire State Plaza, Albany, NY 12228, theresa.egan@dmv.ny.gov.

Via email and U.S. mail

DEAR MR. SCHROEDER AND MRS. EGAN: On June 17, 2019, the State of New York (New York) enacted the Driver's License Access and Privacy Act (the Act), effective December 14, 2019.[1] The Act forbids New York Department of Motor Vehicles (DMV) officials from providing, with very limited exceptions, pertinent driver's license and vehicle registration information to the United States Department of Homeland Security (DHS). Specifically, this Act precludes U.S. Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) from accessing and validating pertinent information contained in New York DMV records that is operationally critical in DHS's efforts to keep our Nation secure. The Act also threatens to block access to other State law enforcement agencies and departments if those agencies or departments provide New York OMV records to CBP and ICE.

Over the years, CBP has utilized New York DMV records in several ways to promote national security and to enforce Federal customs and immigration laws. Having access to New York DMV information has enabled CBP to validate that an individual applying for Trusted Traveler Programs (TTP) membership qualifies for low-risk status or meets other program requirements. An individual's criminal history affects their eligibility for TTP membership. TTP permits expedited processing into the United States from: International destinations (under Global Entry); Canada only (under NEXUS); and Canada and Mexico only (under SENTRI). TTP also allows quicker processing for commercial truck drivers entering or exiting the United States (under FAST). Furthermore, CBP has needed New York DMV records to establish ownership and thus to determine whether a used vehicle is approved for export.

The Act prevents DHS from accessing relevant information that only New York DMV maintains, including some aspects of an individual's criminal history. As such, the Act compromises CBP's ability to confirm whether an individual applying for TTP membership meets program eligibility requirements. Moreover, the Act delays a used vehicle owner's ability to obtain CBP authorization for exporting their vehicle.

Furthermore, on a daily basis, ICE has used New York DMV data in its efforts to combat transnational gangs, narcotics smuggling, human smuggling and trafficking, trafficking of weapons and other contraband, child exploitation, exportation of sensitive technology, fraud, and identity theft. In New York alone, last year ICE arrested 149 child predators, identified or rescued 105 victims of exploitation and human trafficking, arrested 230 gang members, and seized 6,487 pounds of illegal narcotics, including fentanyl and opioids.[2] In the vast majority of these cases, ICE relied on New York DMV records to fulfill its mission. ICE also needs New York DMV information to safeguard Americans' financial and intellectual property rights.

New York DMV records have long been used by ICE law enforcement personnel to verify or corroborate an investigatory target's Personally Identifiable Information (PII), which can include their residential address, date of birth, height, weight, eye color, hair color, facial photograph, license plate, and vehicle registration information. Moreover, ICE's expeditious retrieval of vehicle and driver's license and identification information has helped identify targets, witnesses, victims, and assets. ICE has used DMV records to obtain search warrants, and DMV records are also critical for ICE to identify criminal networks, create new leads for investigation, and compile photographic line-ups. Additionally, during the execution of search-and-arrest warrants, ICE officers have used DMV information to identify individuals whose criminal history renders them a threat. The Act prohibits the sharing of vehicle registration information, including the identity of the person to whom the vehicle is registered, with DHS. That prohibition prevents ICE from running license plate searches, even when ICE is aware that the vehicle's owner has committed a heinous crime. In short, this Act will impede ICE's objective of protecting the people of New York from menacing threats to national security and public safety.

Although DHS would prefer to continue our long-standing cooperative relationship with New York on a variety of these critical homeland security initiatives, this Act and the corresponding lack of security cooperation from the New York DMV requires DHS to take immediate action to ensure DHS's efforts to protect the Homeland are not compromised.

Due to the Act's negative impact on Department operations, DHS will immediately take the following actions:

(1) Trusted Traveler Programs—Global Entry, NEXUS, SENTRI, and FAST.—

Because the Act prevents DHS from accessing New York DMV records in order

[1] N.Y. Veh. & Traf. § 201 (2019).

[2] Nation-wide, last year ICE arrested nearly 4,000 child predators, identified or rescued 1,400 victims of exploitation and trafficking, arrested 3,800 gang members, and seized 633,000 pounds of contraband, including fentanyl and opioids.

to determine whether a TTP applicant or re-applicant meets program eligibility requirements, New York residents will no longer be eligible to enroll or re-enroll in CBP's Trusted Traveler Programs.

(2) Vehicle Exports.—Because the Act hinders DHS from validating documents used to establish vehicle ownership, the exporting of used vehicles titled and registered in New York will be significantly delayed and could also be costlier.

These actions are the result of an initial assessment conducted by DHS. We will continue to review Department-wide operations related to New York to assess and mitigate the Act's adverse impact on national security and law enforcement.

Sincerely,

CHAD F. WOLF,
Acting Secretary.

Mr. KATKO. Thank you.

Could you just briefly summarize the contents of this letter? Then I have a follow-up question for you.

Mr. WAGNER. So my understanding is New York State because of the law that they passed, you know, without consultation shut off the access to motor vehicle data, which included driver's license information, license plate registration, vehicle registration information.

So in our operations, any of the work that we do where we would use that information to help validate an identity, an address, and a vehicle, the ownership of a vehicle is impacted by not being able to do that directly, and the breadth of our mission goes way beyond, I think, what the law says about immigration enforcement.

You are impacting the Customs mission and the National security mission, and all the other areas in which we operate.

Mr. KATKO. Is there any other State in the country that is having this problem with Customs?

Mr. WAGNER. We have worked some other agreements with other States to continue to access the data for, you know, the work that we do.

Mr. KATKO. So am I to understand that New York State is the only one who forbids Customs and Border Protection as well as ICE to have access to their driver databases?

Mr. WAGNER. Yes. It is the only one I am familiar with right now.

Mr. KATKO. Even California?

Mr. WAGNER. California, we have a separate agreement with where we continue to access their information.

Mr. KATKO. Now, I just want to note further as long as we have a couple of minutes here some of the things that are in the letter. Tell me if this is correct.

On a daily basis, ICE uses New York DMV data in an effort to combat transnational gangs, narcotics smuggling, human smuggling and trafficking, trafficking of weapons and other contraband, child exploitation—child exploitation?—exploitation of sensitive technology, fraud, and identity theft.

Is it fair to say that by not having access to the database, it hampers those investigations at times?

Mr. WAGNER. Sure. Any law enforcement practice where you would normally use that information, yes, would be impacted.

Mr. KATKO. I yield back the balance of my time.

Chairman THOMPSON. Thank you.

The Chair recognizes the gentlelady from New York, Miss Rice, for 5 minutes.

Miss RICE. Thank you, Mr. Chairman.

Let's continue, Mr. Wagner, if we can, talking about what happened with New York.

Was CBP made aware of the policy before the Acting Secretary's announcement on Fox News?

Mr. WAGNER. Yes.

Miss RICE. So you were aware of it. No notification was made to Congress about blocking access to these Federal programs for New Yorkers?

Mr. WAGNER. I do not know.

Miss RICE. Well, there was none.

So personally, we, my office has already received an influx of new questions about this policy literally overnight. Fifty to 80,000 New York State residents are affected who have pending global entry enrollment applications or renewals.

This is going to have an enormous impact on people, many of whom entered into this program because their jobs require them to travel internationally.

So what do you plan to do about all those people who are going to be impacted?

Mr. WAGNER. Well, without the ability to help validate their identity through the——

Miss RICE. You have their fingerprints.

Mr. WAGNER. Yes, but if they have not been arrested, the fingerprints do not tell us anything. What would the fingerprints tell you if you have not been arrested?

Miss RICE. So what are you trying to find out is my point.

Mr. WAGNER. Trying to validate their address where they live, their residency. These are things important to us as we establish that low-risk Trusted Traveler status that we afford people in that program. Without the ability to do that, how would we do that?

So New York State shut off without consultation our access to that information in December. How would we continue to operate and validate who people are?

Miss RICE. Well, going forward, what about the people who already have it?

I have global entry. So when I go to renew it, I am not going to be able to do that.

Mr. WAGNER. Correct.

Miss RICE. Yet here I am, a sitting Congresswoman with global entry. So to me, to me, to me, I understand the distinction that you are making. There are at least 15 other States you are saying that you have individual agreements with all of them where they do not block access to this database? Fifteen other States who have a global——

Mr. WAGNER. I am not aware of any other State blocking our access to that information.

Miss RICE. OK. So I would like you—we are going to follow up. I am going to follow up directly with you because there are at least 15 other States that allow undocumented people to get driver's licenses.

Mr. WAGNER. Yes.

Miss RICE. I would——

Mr. WAGNER. I am not aware of them blocking our information.

Miss RICE. OK. So you not being aware is not a sufficient answer because there could be other States that do, and it seems to me that this is, once again, an attempt by this administration, specifically Donald Trump, who formerly was a New Yorker, to punish New York.

So you and I are going to follow up on this, and I appreciate you trying to answer these questions, but we need more information, and I appreciate your attempt to answer these questions.

I yield back. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much.

Mr. Wagner, just for the record, can a person have global entry without a driver's license?

Mr. WAGNER. Yes, I believe so.

Chairman THOMPSON. So I am trying to figure out how you are going to cancel all of these people and some of them do not even drive and deny them.

Mr. WAGNER. Well, it is a New York State identification.

Chairman THOMPSON. But they have passports.

Mr. WAGNER. Validation of that information.

Chairman THOMPSON. But they have a passport. They have a passport.

Mr. WAGNER. How do we validate the address of where they live?

Chairman THOMPSON. My driver's license has a post office box. So, I mean, I am just trying to figure out are you being——

Mr. WAGNER. Why is the information blocked for this purpose then?

Chairman THOMPSON. Well, I do not know. I am saying why would you cancel it if it——

Mr. WAGNER. Well, why would New York State block the information for this purpose?

Chairman THOMPSON. Is it for identification or security?

Mr. WAGNER. Both.

Chairman THOMPSON. But you can prove it with other documents. I mean, that is what I am trying to figure.

Well, the Chair recognizes the gentleman from Louisiana, Mr. Higgins.

Mr. HIGGINS. Thank you, Mr. Chairman.

I yield 1 minute to my colleague, Mr. Katko.

Mr. KATKO. Thank you, Mr. Higgins.

Just have a quick follow-up question with my colleague, and it is a quite simple one really.

First of all, it is clear that it hampers investigations with ICE. It is clear that it hampers the ability to get certain identification that is available in driver's DMV database in New York State.

I just want to make sure that it is clear. My colleague from New York, Miss Rice, mentioned that there are many other States that have possible—like allowing illegal aliens to get driver's licenses.

That is not the issue. The issue is, is there any other State in the United States of America that completely blocks Customs and Border Protection and ICE's access to DMV records.

Mr. WAGNER. I do not believe so.

Mr. KATKO. OK. So in my opinion, and I have an immense amount of respect for my colleague from New York, I do not believe this is a political exercise. All New York would have to do is enter into a similar agreement that those other 15 States have entered into with Customs and Border Protection and ICE where they simply verify that they will not use it for immigration enforcement purposes, but use it for law enforcement purposes and for global entry and those types of things.

Is that correct? You can do that?

Mr. WAGNER. I think that is a discussion we would have with the State.

Mr. KATKO. OK. You have done it with other States?

Mr. WAGNER. Yes.

Mr. KATKO. OK. Thank you.

I yield back.

Mr. HIGGINS. I thank my colleague.

Just to follow up on the New York question because it is just a fascinating topic, are you aware of negotiations or communications prior to the New York legislative body passing this law with Customs and Border Protection?

Were we out front with this communication at all?

Mr. WAGNER. Our access——

Mr. HIGGINS. It seems to me like they should have known before they passed the law this was going to happen.

Mr. WAGNER. Right. Our access was just turned off one day in December, and our officers and agents in the field called in and said, you know, "What happened to our access?"

Mr. HIGGINS. So you are saying that as far as you know, and you can certainly advise if you do not know or have no way of knowing, but as far as you know, sir, was there an on-going communications during the course of the development of this legislation in the State of New York with the law enforcement agencies like Customs and Border Protection and ICE?

Mr. WAGNER. I do not know. I am not aware of any.

Mr. HIGGINS. Well, one would hope that there was.

Dr. Romine, you mentioned black box texting. Would you clarify that that means that as your products are tested through NIST, your facial recognition products provided by vendors, that they are tested without your knowledge of who the vendor is? You are strictly looking at the results of the algorithms themselves?

Mr. ROMINE. So when I use the phrase "black box testing," what I mean is that we do not have any insight into the characteristics of the algorithm itself. We publish an API, an application——

Mr. HIGGINS. Do you know the identity of the vendor?

Mr. ROMINE. It is self-identified.

Mr. HIGGINS. It is self-identified as you are studying the product itself.

Mr. ROMINE. That is correct. We do that.

Mr. HIGGINS. OK. Just to clarify that.

Now, can any vendor submit an algorithm to NIST for testing?

Mr. ROMINE. Yes, sir.

Mr. HIGGINS. The process by submitting that product is standardized?

Mr. ROMINE. It is, sir.

Mr. HIGGINS. All right. With the top-performing algorithms like Customs and Border Protection uses, is there a wide variance between what you are referring to as the top-performing algorithms and, say, academic projects perhaps submitted for testing?

Mr. ROMINE. Yes, sir. There is a wide variance in the performance of algorithms at the top.

Mr. HIGGINS. So in your scientific assessment of NIST testing and evaluation of facial recognition technologies, would you say that what we are referring to as the top-performing algorithms that are being used by Customs and Border Protection are far and beyond some of the common products that are presented to you?

Mr. ROMINE. The top-performing algorithms are significantly better in their error rate.

Mr. HIGGINS. Can you confirm for this committee, sir, that it is, indeed, the top-performing algorithms at this point that are being used by Federal law enforcement agencies?

Mr. ROMINE. Sir, I have no way to independently verify that.

Mr. HIGGINS. But would you say that Customs and Border Protection is using the top. I want to confirm.

Mr. ROMINE. I did not say that.

Mr. HIGGINS. Can you confirm that, good sir?

Mr. ROMINE. We are using not the algorithm they tested, but we are using the previous version of it, and we are switching to, we are upgrading to the version that they tested next month.

So, yes, we are using a high-performing vendor.

Mr. HIGGINS. Going to the next iPhone? All right. I think that vaguely answers my question, and my time has expired.

Mr. Chairman, thank you.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the gentleman from New Jersey, Mr. Payne.

Mr. PAYNE. Thank you, Mr. Chairman.

Let me ask. Who and where is all of this facial recognition data stored?

Please describe under what specific circumstances this data is allowed to be shared or used or transferred, if that is the case?

Mr. WAGNER. We are using as a database travel document databases. So these are photographs collected by the U.S. Government for the purposes of putting on a travel document, like a U.S. passport or a U.S. visa that is issued to a foreign national or a photograph of a foreign national when they arrive in the United States, like under the Visa Waiver program.

We would take their photograph or read the photograph from the chip in their passport and store that. That is what forms the baseline gallery that we match against.

Now, new photographs we take of a person, U.S. citizen, if we match it to a U.S. passport or a U.S. identity, those photos are discarded, OK, after 12 hours just for some system work.

If you are a foreign national, that goes over to a system called IDENT that DHS runs where they are stored under the protocols of the Systems of Record notice of the data retention period of that, which I believe is 75 years.

Mr. PAYNE. OK. All right. To follow up with that, you know, we are living in an age where everything is being hacked. What type of security measures or protections have been put in place regarding the security of this data?

Mr. WAGNER. So the databases are housed within the U.S. Government. CBP does not necessarily keep or own any of those permanent databases. You know, they are owned by Department of State. They are owned by other branches of DHS.

We access a lot of that information. We use it. We match against it, and then we put information back into them.

Mr. PAYNE. OK. You know, I continue to have hits come across my desk about the mishaps and disadvantages of facial recognition technology and the racial bias. It is my understanding that the technology continues to misrepresent and irregularly identify people of color and women.

So am I hearing from the majority of the panel that that is not the case? Because it keeps coming to us. So there has to be some validity.

Mr. ROMINE. Sir, in our testing for the one-to-one identification algorithms, we do see evidence of demographic effects, differences with regard to race and sex and age.

Mr. PAYNE. OK.

Mr. ROMINE. In the one-to-many identification testing that we did for the algorithms that we tested, there was a small set of high-performing algorithms that had undetectable differentials.

Mr. PAYNE. OK.

Mr. ROMINE. But the majority of the algorithms still exhibit those characteristics.

Mr. PAYNE. Can you give a description of the difference between the two sets?

Mr. ROMINE. Yes, sir. In the case of verification, verifying an identity, a biometric is matched solely or in the case of face recognition a picture is matched against——

Mr. PAYNE. Is that the one-to-one?

Mr. ROMINE. That is the one-to-one.

Mr. PAYNE. All right.

Mr. ROMINE. The identification or the verification is to try to determine if you are who you say you are.

Mr. PAYNE. All right.

Mr. ROMINE. It is matched against a gallery of one, in essence.

Mr. PAYNE. What is the one-to-many?

Mr. ROMINE. The one-to-many is matched, in the case of CBP's application, one to perhaps thousands for the airline public, the traveling public, or one to millions in the case of law enforcement, such as FBI, to try to identify a suspect.

Mr. PAYNE. So you are saying that the percentage of identifications in the one-to-one, you have more incidents of this bias that we see?

Mr. ROMINE. I should clarify. In the algorithms that we tested, that is correct. However, many of the vendors who chose to participate in the one-to-many testing did not choose to participate in the one-to-one, and those are some of the highest-performing in the one-to-many.

Mr. PAYNE. OK. Thank you.

I yield back, Chairman.

Chairman THOMPSON. Thank you.

The Chair recognizes the gentleman from North Carolina, Mr. Walker.

Mr. WALKER. Thank you, Mr. Chairman.

I would like to yield 1 minute to the gentleman from Louisiana.

Mr. HIGGINS. Thank you, my colleague.

Dr. Romine, I have a question regarding the effectiveness of the technology that you have tested regarding children.

Is it a potential if we assembled a gallery of photographs of children crossing the border, some of whom are being exploited and false identifications presented; how does the technology work with children compared to mistake and errors in other demographics?

Can this technology be used to protect children that are perhaps being exploited crossing our borders, coming into our country?

If so, what can we do to protect the privacy of those children, given the fact that they are minors?

I will leave you my remaining 30 seconds here.

Mr. ROMINE. Thank you, sir.

The application specifically is something that we do not test. What we have tested is the effectiveness of the algorithms in terms of error rates.

We do find that for children in the one-to-one setting, the one that you just described, there are demographic effects there. There are differentials. The error rates are higher in the one-to-one case with respect to age.

So it is more difficult. Based on our testing, it appears more difficult to match.

Mr. HIGGINS. But there is no gallery. There is no one-to-many. There is no gallery of the photographs that you have.

Mr. ROMINE. We have no such gallery.

Mr. HIGGINS. If we did develop that, then NIST could test the effectiveness and perhaps this could be a tool to protect children?

Mr. ROMINE. We could. We could undertake many different kinds of testing to determine the effectiveness of those.

Mr. HIGGINS. Thank you, sir.

I thank my colleague for yielding.

Mr. WALKER. Absolutely. Thank you, Representative Higgins.

Mr. Wagner, is it true that a biometry entry/exit system uses less personally identifiable information than the current system that we have in place?

Mr. WAGNER. Yes, because currently you open your passport booklet and show it to an individual to either, say, check your bags, go through TSA screening, board the plane, a CBP officer. You are exposing your name, your date of birth, your passport number, your place of birth, all the information on your passport page.

Somebody could be looking over your shoulder. Somebody could take a picture over your shoulder looking at that. You are disclosing it to a person who does not actually need to know all of that additional information versus standing in front of a camera with no identifiable information other than your face, which they can already see, and your picture is taken and on the screen comes a green checkmark, and that person now knows you have been validated by the Government record to proceed.

So you are sharing actually less information in this instance.

Mr. WALKER. But not only sharing less information, but on a scale of 1 to 10, 10 being the highest, how would you rate this progress as, in your own words, continuing to develop and right-fully so, would be the highest security possible for travelers compared to anything else that we are doing now?

Mr. WAGNER. Right now I think on top of everything else we are doing, it brings us closest to 10, which is where we want to be.

Mr. WALKER. When Representative Higgins talked about some of the children involved, are there any numbers or statistics based on people that you have caught either involved in human trafficking or some other nefarious activity because, strictly because of the facial recognition?

Mr. WAGNER. Yes. On the land border, we have got 247 imposters so far, meaning they had a legitimate document that belonged to somebody else. Eighteen of those, so 7 percent, were under the age of 18. So they would be considered children.

Seventy-three of those at the land border had U.S. passports or U.S. passport cards, and 46 of them, or almost 20 percent, had criminal records that they were trying to hide.

Mr. WALKER. Do you believe these were identified strictly because of the use of facial recognition or was there any other aspect or involvement?

Mr. WAGNER. Our officers are also very good at identifying the behaviors in the person when they present the travel document. A lot of times that can also be a cue that the person's hiding something.

But the technology on top of officer's skills and abilities should bring us to that security posture that will bring us to near perfect.

Mr. WALKER. Are there any policy's difference between a U.S. citizen versus non-citizen?

Mr. WAGNER. Well, everyone has to establish their identity by law. Everyone has to produce some type of identification. The law requires a U.S. citizen to travel on a passport.

Mr. WALKER. In the process, scrubbing this 12 hours after is what?

Mr. WAGNER. That is our internal policy. We take a new picture. We discard it after 12 hours. We are looking at actually shrinking that to a less time. We only keep it there in case the system crashes and we have got to restore everything.

Mr. WALKER. Thank you, Mr. Wagner.

I yield back, Mr. Chairman.

Chairman THOMPSON. Thank you.

The Chair recognizes the gentlelady from Las Vegas, Ms. Titus.

Ms. TITUS. Thank you, Mr. Chairman.

I find this interesting. The more you talk the less I know, it turns out, unfortunately.

McCarran Airport is in my district. It is a very busy airport, one of the busiest in the country. A lot of international tourists come through there.

So I know we have talked a lot about the use of this facial recognition for security reasons. I would like to talk about it in terms of how it affects the passengers' experience. We want people in Las Vegas to have a good experience from the time they land until the time they leave.

So how do you work to coordinate using this for security and also reducing wait times or serving the passenger as opposed to making it more difficult for the passengers?

Mr. Wagner.

Mr. WAGNER. So it absolutely supports our travel and tourism goals as well. It makes a much better passenger experience, a more convenient passenger experience, a more consistent passenger experience.

You think as you go through the airport the number of stops you have to make to produce a piece of paper or open your passport again or provide some other form of validation to go forward.

You can use the facial recognition and the camera to have that same process. It is quick enough that you walk up and your picture is taken and 2 to 3 seconds you are moving forward.

So what we are seeing is reduced wait times. The airlines as they incorporate it into the boarding process are reducing their boarding times over the aircraft sometimes as much as, say, 40, 45 percent.

It is a different atmosphere for the travel because you are not fumbling for your documents or forgetting where you put your boarding pass or getting stuck in line behind the person whose phone went dead when they went through to read their boarding pass or forgot where they put their passport.

So it is creating a better atmosphere for the traveler. It is moving the lines quicker because you cannot leave your face on the plane. You cannot, you know, leave your face in the bathroom. You cannot forget that like people do with their travel documents.

So it is making an easier process because everybody knows how to take a picture, and what we see is people are enjoying this process a lot better for them, and what we are seeing is the lines reduced.

Ms. TITUS. Are you working with TSA or local law enforcement to make this all run smoothly or is that not necessary?

Mr. WAGNER. So we are working very closely with TSA. We have run a few pilots with them. We have an on-going pilot in Atlanta because we build the gallery as the person prints out their boarding pass. So anyplace now where they have to show their passport at the airport, say, when they are departing the United States, you could take a picture and validate it against our gallery.

So you are outside of the airport or you just walked into the airport. You got your boarding pass. Your picture goes into that gallery.

So steps like checking your bags where you have to show your ID to the airline person, you can have a camera there that does that.

You go up to the TSA checkpoint. TSA can take a photograph. It transmits to our gallery, again, because we built it for the biometric exit requirement, but we want to make that environment available to all the other places in the airport where you would show your passport to do that.

So, yes, so for TSA you could take a picture. Then you go through screening. You go to board the plane. The airline takes your picture. It comes back to our gallery. We confirm it. You can board the plane without even showing your passport to the airline or showing your boarding pass to the airline.

Ms. TITUS. Well, suppose you find somebody does not match. My understanding is this goes through an app, and law enforcement, if they are busy or if the person responsible for checking out the non-match is doing something else, do you have some kind of staffing model for who is responsible for that?

Because I had heard it comes through an app, and since there is no action that you are supposed to take that is very clear, sometimes they just ignore it.

Mr. WAGNER. Depending on where you are in the airport, generally it would be the airline or CBP, we would just look at the physical passport, which is what you are presenting now, and we would make a determination.

Now, if we have doubts about do you match the picture on your passport, right, which happens, or if the airline has doubts you match the picture on your passport, they may call us over. We may ask the person for another form of ID. We may ask them additional questions. We may do a further inspection on them.

So if you do not look like your passport photo, you know, from a visual review, these are the same kind of things that would occur.

Ms. TITUS. We have been having a lot of confusion about going to the Real ID from just regular driver's licenses. People do not know they have to do that. We are trying to get the word out.

Some States did not provide the funding to go to Real ID. Is that transition part of your consideration as you develop this new system or is it not connected?

Mr. WAGNER. It is separate than this.

Ms. TITUS. So that it is not going to make any difference?

Mr. WAGNER. Not really.

Ms. TITUS. All right. So people who will use their passports instead of Real ID, that will not matter?

Mr. WAGNER. Right, because these are international travelers we are talking about today. So they would generally have a passport.

Ms. TITUS. You do not see this moving to national as well as international once it is up and running?

Mr. WAGNER. I would defer to TSA on that for their requirements on how this might apply to a domestic flight.

Ms. TITUS. OK.

Mr. WAGNER. I think there is some good discussion to have there, that if people have passports and you could electronically confirm them, even on a domestic flight, should the traveler opt into this, I think it would be good government to build a system like this if that is what people would want.

Ms. TITUS. Well, thank you.

Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you.

The Chair recognizes the gentlelady from Illinois, or I am sorry. The gentleman from Texas, Mr. Crenshaw.

Mr. CRENSHAW. Thank you, Mr. Chairman.

Thank you all for being here. It has been an interesting hearing to watch.

I just want to dispel any misinformation on the facial recognition technology that we are discussing here today. It seems to be abnormally controversial.

We are not talking about 1984-style Government surveillance, not like China has. We are not talking about facial recognition at the National Mall or Times Square or downtown Houston.

We are talking about facial recognition at air, land, and sea ports of entry, where the Government has not just the authority but the duty, the responsibility to know who enters our country and where they are already checking for identification, of course.

It seems from the answers we have gotten that CBP is using the best algorithms with almost no bias whatsoever in them. That is what we have established today as far as I understand.

Locations where facial recognition technology is employed, those locations are marked, correct?

Mr. WAGNER. Yes. It is where you would normally present your passport.

Mr. CRENSHAW. OK. Locations where facial recognition technology is employed where entrants are required to present, and you already answered that one, present a form of photographic identification already.

Entrants are allowed to opt out of facial recognition technology and present photographic identification to a CBP officer who will then compare the physical appearance of the entrant and the photographic identification presented, correct?

Mr. WAGNER. Correct.

Mr. CRENSHAW. Biometric data for U.S. persons is stored for no more than 12 hours in an encrypted virtual private cloud, correct?

Mr. WAGNER. Correct.

Mr. CRENSHAW. Biometric data for entrants who are not U.S. persons are stored in IDENT, correct?

Mr. WAGNER. Correct.

Mr. CRENSHAW. Giving the above and knowing where facial recognition technology is used, requirement to present photo ID, the ability to opt out, and a secured storage, what are the major privacy concerns I might be missing?

How can we improve this?

Mr. WAGNER. I think what we have heard from the privacy community is people get used to the convenience of this technology and that bleeds over into the commercial world or their private sense, and they may be more likely to allow that to happen outside of the Government requirements.

You know, in my discussions with them, I said, "Yes, but there is also an expectation by the public that they have this convenience in their private life and why should their interactions with their Government be so antiquated?"

Mr. CRENSHAW. Yes.

Mr. WAGNER. Why should their travel through the airport be so antiquated and manual and frustrating?

You know, do they not expect that that same convenience should apply when they are traveling internationally?

Mr. CRENSHAW. One way this could be viewed in a very positive sense is to combat human trafficking. Is there a way that tools like this can be integrated with other tools like Spotlight and SAFER to battle child sex trafficking, human trafficking?

Mr. WAGNER. Sure. Because what this helps us do is our core vetting processes are biographically-based, right? A name and date of birth is submitted, say, to a watch list, you know, through an airline application, through TSA, and we vet and do those background checks on the basis of, say, who the airlines tell us who is flying, so who checked in, who purchased a ticket.

But when you can then use a biometric to validate that you vetted the right person, you have the assurances that that is the person who is actually traveling and not just their passport is traveling under a different person that is being trafficked.

So it helps us close those vulnerabilities of imposters for nefarious or being trafficked or being victimized to be able to do that using imposter documents.

Mr. CRENSHAW. In my limited time left, can this be used to combat visa overstays as well?

Mr. WAGNER. Yes. Now, we track visa overstays primarily through the biographic information the airline provides, but by implementing this system, we have actually biometrically confirmed almost 44,000 by overstays. With the biometric validation that these people overstayed, they end up leaving the United States, albeit late, later than they were authorized to do so. So, you know, just about 44,000.

Mr. CRENSHAW. Thank you. I yield back.

Chairman THOMPSON. Thank you.

The Chair recognizes the gentleman from New York, Mr. Rose.

Mr. ROSE. Thank you, Mr. Chairman.

Mr. Mina, the NYPD has in the past used facial recognition to compare photos from crime scenes against its own internal arrest databases. Some State lawmakers want to take that ability away from the NYPD and other New York State law enforcement agencies.

Do you support police agencies using facial recognition in the course of their criminal investigations?

Mr. MINA. Congressman, that is not necessarily an issue that we have looked at at CRCL. We are primarily looking at the DHS uses of facial recognition technology and, in particular, we have focused primarily, as Dr. Romine mentioned, less so on the identification piece where you have sort-of you are trying to match a photo to a gallery of, you know, tons, and we are looking at a much narrower. We are looking at, I think, more of the verification, if I understand the technology correctly.

Again, our role there is really to make sure that we are addressing these concerns regarding impermissible bias, whether that is, again, based on race, national origin, age, gender, as we have talked about.

Mr. ROSE. So one thing that I think has been absent in this conversation is the ways in which civil liberties can potentially be infringed upon in the absence of the use of technology. Can you speak to this for a minute or two?

I am thinking of false positives. I am thinking of people who are being arrested or at least questioned further based off of just a verbal description.

Mr. MINA. Absolutely, Congressman. So I think that it is obviously critically important to blend both the use of technology as well as the end-user in this process.

I do not think it is an either/or proposition, and as we have advised CBP and other DHS components, that is, from a policy-making perspective, that is really where we see the greatest benefit, is really that interaction between the technology and the user.

Because, as Mr. Wagner talked about earlier, for example, if there was a false negative, for example, then you would have the line officer looking or agent looking at their actual, you know, passport or other travel documentation and making that independent verification.

Mr. ROSE. Sure.

Mr. MINA. Then if it matches, the person goes along and they board the flight.

Mr. ROSE. Right. I think that it is important to know then so that we are all on the same page that the use of technology has consistently been implemented to preserve our public safety, but also to further protect civil liberties.

This is being lost in this conversation as yet again I think we are unnecessarily politicizing an effort to keep us safe.

It is not perfect, and you all have some work to do to make it even better, and I am encouraged to hear that you are making it better.

Mr. Wagner, you are going to have to hear from another New Yorker. So look. I am not a supporter of this New York legislation that was passed. I think it is unfortunate and wrong that you all were not notified, but two wrongs do not make a right.

So I am going to ask some very simple questions. If you all were setting out to be the professional force that you are and do this professionally, do you think that in advance of announcing this you should have told Congress what was wrong and what would happen if it was not fixed or addressed?

Mr. WAGNER. I would have to defer to DHS on that.

Mr. ROSE. No. Come on, man. This is ridiculous. It is a simple question. That is a simple question.

We heard about this from Fox News. This is politics at its worst. We are talking about acting like professionals right now.

If there is a problem that needs to be addressed and you all are doing this, do you think it was appropriate that we were not told well in advance so we can try to arrive at some solution?

Do you think that is OK? Is that the way you would want to carry this out?

Mr. WAGNER. I am not going to comment on that. I mean, that is your——

Mr. ROSE. You are not going to comment. So by the fact that you have given very clear and declarative answers previously, I think that we can all assume what you are thinking and unwilling to say right now.

So let's commit to actually trying to solve problems here. You have got Members of Congress that will not be able to renew something. You have got more important than Members of Congress. Who cares about Members of Congress? Millions of other people that are now held in the balance, people on my staff, people, colleagues, all types of people, all types of people.

This is politics. If you really were making an effort to address a problem, to address a problem, there would have been a system, a proposal, a negotiation, a conversation, letters written. That is the way business is conducted.

So let's put that aside. Would you now commit, now that we have all engaged in our politics, to actually having sensible meetings and conversations about a way forward to solve this issue?

Mr. WAGNER. Sure, I think that is a good point.

Mr. ROSE. You would commit to that. OK. Thank you.

Chairman THOMPSON. The gentleman's time has expired.

The Chair recognizes the gentlelady from Illinois, Ms. Underwood.

Ms. UNDERWOOD. Thank you, Mr. Chairman.

Many of my constituents in Northern Illinois have to drive over an hour to get to a major airport in Chicago and, therefore, we are always interested in learning more about technologies that can improve airport security wait times, but biometric data is ripe for potential abuse and misuse, which is why it is so important to ensure that DHS uses facial recognition and other technologies in a fair and reliable and effective way.

Mr. Wagner, although children under the age of 14 are not required to be screened, many do go through screening that collects their biometric information.

How does CBP store and secure this information? I am talking about under 14.

Mr. WAGNER. I think if you are outside the scope of the biometric tracking requirement, which is 14 to 79, I believe we discard all of that information. Let me verify that.

Ms. UNDERWOOD. Yes. Would you be willing to provide the committee with that information in writing?

Mr. WAGNER. Yes.

Ms. UNDERWOOD. Both the procedure and the policy in order to do so?

Mr. WAGNER. Yes.

Ms. UNDERWOOD. OK. Are there any differences in how CBP collects, uses, or secures children's biometric information in comparison to adults?

So if a child presents, does it take it and immediately release, right, or is it going to be going through some kind of filtering later on?

We want that level of information.

Mr. WAGNER. OK. You have got it.

Ms. UNDERWOOD. OK. The December 2019 NIST report found that children are more likely to be misidentified during biometric screening.

Of course, we know that other groups, like we have discussed today, people of color, seniors, are also misidentified.

Mr. Wagner, what actions is CBP taking to correct the patterns of errors identified in the NIST report?

Mr. WAGNER. Well, again, we are using a high-performing algorithm that we are not seeing those demographic-based error rates.

Now, if someone does not match to either the gallery or to the document they are presenting, we will physically examine the document.

Ms. UNDERWOOD. Right.

Mr. WAGNER. Manually look at the picture, and if we have the confidence it is the person, we can do that through questioning. We could do that through additional forms of identification. We can do that through an inspection of the person.

Sometimes it is just looking at the passport and going, "OK. That is you. Go ahead."

It all depends on how discrepant you look from your travel document photograph.

Ms. UNDERWOOD. Some passengers report being unaware or confused about how to opt out of their biometric screening. As CBP expands the biometric screening program, does it intend to reevaluate the best method of communicating the important opt out information to passengers?

Mr. WAGNER. Yes. So right now we have got signage at the airports, but you know, a lot of people do not read signs at the airport.

We have got gate announcements that the airlines try to make before boarding, but again, there is always competing announcements going on, and sometimes it is tough to understand what is being said.

So we are actually looking with the airlines as could we print things on the boarding pass.

Could we give notifications when they are, say, booking their ticket or when they are getting their check-in information for boarding?

Are there electronic messages we could provide?

Ms. UNDERWOOD. Right.

Mr. WAGNER. So we are looking at additional ways to do that.

We also started taking out some privacy advertisements advising people of the requirements and what their options are as well, too.

Ms. UNDERWOOD. OK. Well, it is certainly my interest in making sure that every passenger understands that, No. 1, this is happening and, No. 2, that they have a choice to opt out, and I would certainly urge the CBP to strongly consider and issue this committee a time line for perhaps outlining how we can improve that communication to all passengers.

Does CBP capture and report the rate of false positives or mistaken identifications among different demographics at each port of entry where biometric technology is used?

Mr. WAGNER. What we track are the people that we take a photograph of or receive a photograph of.

Ms. UNDERWOOD. Right.

Mr. WAGNER. And we are not able to match it to their travel document that is in our gallery.

Ms. UNDERWOOD. Right.

Mr. WAGNER. Again, that is that 2 to 3 percent.

Our review of that information does not show noticeable discrepancies on any types of——

Ms. UNDERWOOD. That was not my question. My question is capturing and reporting by port of entry. So we want to know the false positives. Are we seeing more at certain places along the border?

Are we seeing more false positives at certain airports?

Mr. WAGNER. We are not seeing false positives that is matching you to a different identity. We are not seeing that with this technology.

Ms. UNDERWOOD. Or mistaken identities?

Mr. WAGNER. We are not seeing that. We are more likely you do not match against anything. So we get a no information return.

Ms. UNDERWOOD. OK. Dr. Romine, can you elaborate on what NIST recommends to algorithm developers to improve accuracy across demographics?

Mr. ROMINE. The report, the testing that we do does not result in recommendations specifically to the vendors other than to take the data that we provide, the evaluation results, and strive to use those results to improve their methods. But——

Ms. UNDERWOOD. So you are saying that you do not have a lot of interaction with the developers?

Mr. ROMINE. We have informal interaction with them in the sense that the scientists who do this biometric testing are part of a larger biometrics community. We see the vendor representatives, the scientists at meetings, and so on.

But with regard to the FRVT itself, the testing, the feedback that we provide to the vendors is the test result.

Ms. UNDERWOOD. OK. So you all are not doing like convenings with industry and helping them improve the quality of their product?

Mr. ROMINE. We do host events, but more as a convener to get the community together to discuss different techniques. But we do not provide, other than sort-of in the general scientific community sense, we do not provide specific recommendations for their improvement.

Ms. UNDERWOOD. OK. I recognize my time has expired. We would just like to get more information about that in writing.

Mr. ROMINE. Happy to do that.

Ms. UNDERWOOD. Thank you, sir.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the gentlelady from New Jersey, Mrs. Watson Coleman.

Mrs. WATSON COLEMAN. Thank you, Mr. Chairman.

Thank you for your testimony.

A couple of questions. I think I want to just talk more about the role of the CRCL and NIST. It seems to me that there has not been much coordination across the DHS spectrum of directions from DHS to each component regarding their deployment of biometric technologies. You can correct me if I am wrong.

Is there any sort of Department-wide strategy in place for the use of biometric technologies or are components like yours given wide latitude to stand up biometric programs as you please?

Mr. WAGNER. I am sorry?

Mrs. WATSON COLEMAN. Are you a Lone Ranger?

Mr. WAGNER. Are we what? I am sorry. I did not hear that.

Mrs. WATSON COLEMAN. OK. It does not seem like there is coordination. It does not seem like there is this sort-of Department-wide oversight.

I want to know whether or not you are getting directions from others because then I am going to ask Mr. Mina what is your role and to what degree have you been involved in the oversight and in signing off on how these things are being done.

Mr. WAGNER. Yes. So as we build out new programs, we are bound by certain statutes that require us to publish, say, your Systems of Record notice, your privacy impact assessment, where, you know, things are reviewed by, you know, our internal counsel or our Privacy Officer, and to make sure we make and meet all of the requirements of the statutes.

Do you have the authority to collect what you are doing?

You know, is your time line for storing it and sharing it, is that all permissible in law?

Is it consistent with your mission? Are you authorized to do those things?

Mrs. WATSON COLEMAN. So are you operating within your sort-of silo?

This is what the law says with regard to what you can do. Is this how you execute based upon what your interpretation is of that or is there a DHS component that plays into this as well and says, "OK. But this is how we want to see this"?

Mr. WAGNER. Well, depending on like the acquisition process, there is a multitude of people at DHS that look at the acquisition, the resources spent.

There is a whole process to go through for approval before various boards that authorize the expenditures and the investment in that. There is the DHS privacy officer. There is DHS counsel. So there is a lot of oversight by DHS already in this process.

Certainly the rulemakings would go through with DHS counsel, with DHS policy. So there is a lot of oversight and coordination.

Mrs. WATSON COLEMAN. It is my understanding though that there is no centralized body within the Department that gives the program a stamp of approval or certifies that they are ready for prime time. Is that correct?

Has CRCL approved your program? Do you know?

Mr. WAGNER. No. They would not necessarily go to them for approval, but there is——

Mrs. WATSON COLEMAN. Well, for approval in the sense of maintaining or protecting privacy rights.

Mr. WAGNER. So things are reviewed by them, and I will refer to my colleague.

Mrs. WATSON COLEMAN. What authority do you have, sir, Mr. Mina?

Mr. MINA. Why do I not answer that in a couple of different ways, Congresswoman?

So let me step back a second and talk a little bit about the first part of your question regarding sort-of the enterprise-level review.

I think one of the ways in which CRCL participates in that dialog is by serving on enterprise level-wide working groups across the Department that include representatives from CDP, DHS S&T, and the Office of Biometric Identity Management, where we actually are talking about a lot of these issues.

Now, we do not have a privacy impact assessment type model. However, we do work very closely with the Privacy Office regarding not just facial recognition technology but certainly other forms of biometric identification that the Department uses.

Now, with regard to our relationship with CBP, we work with them in a couple of different ways. First is very, you know, directly in terms of offering them advice and then also we on-site visits and we also work with CBP and the Privacy and Civil Liberties Oversight Board and their engagement as well.

Mrs. WATSON COLEMAN. So is your role anything more than just advice, observation and advice?

You have no authority to say, “No, that is not working. That is a violation.” No, that is it, right? Advice?

Mr. MINA. That is not entirely accurate. What I would say is, yes, we do have an advisory capacity. We also have a compliance function where we do offer recommendations to components based on the——

Mrs. WATSON COLEMAN. If they do not follow them?

Mr. MINA. Then we can elevate it if necessary.

Mrs. WATSON COLEMAN. OK. I have one last question?

Chairman THOMPSON. Yes.

Mrs. WATSON COLEMAN. The question has to do with just the whole system that is used when we are taking pictures and you know.

Who is in charge of determining whether or not the lighting is good, the background is adequate, the cameras are good, they are placed right so that we can get the best pictures that we need to get?

Is there anyone in charge of that?

Mr. WAGNER. CBP would be, and that is going to be based on, you know, our results of, say, the match rates. You know, you can have an airport with a bank of booths and the windows are such that the sunlight comes in and affects these booths during the morning and these booths in the afternoon. Those are the things we have got to look at as we deploy this.

What are the environmental factors that are going to influence all the different locations that we are going to do this?

Then we try to adjust, and that might mean we add more tint to the windows.

Mrs. WATSON COLEMAN. How do you do that? How do you do that?

Mr. WAGNER. We do that internally by reviewing the data and the results of what happens.

Mrs. WATSON COLEMAN. On what kind of a basis? Weekly? Daily? Monthly? Whatever.

Mr. WAGNER. All of it.

Mrs. WATSON COLEMAN. You know what time the sun comes in that window, and you know what time the sun comes in that window.

Mr. WAGNER. Right. I would say we do it continuously to get the best production we can out of it.

Mrs. WATSON COLEMAN. Thank you. Thank you very much.

Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the Ranking Member.

Mr. ROGERS. Thank you, Mr. Chairman.

I have a unanimous consent request that two articles on this topic be admitted to the record.

Chairman THOMPSON. Without objection, so ordered.

[The information follows:]

White Paper by Security Industry Association

WHAT NIST DATA SHOWS ABOUT FACIAL RECOGNITION AND DEMOGRAPHICS

By: Jake Parker, Senior Director of Government Relations, Security Industry Association, jparker@securityindustry.org

INTRODUCTION

In December 2019, the National Institute of Standards and Technology (NIST) published the most comprehensive report[1] to date on the performance of facial recognition algorithms—the core component of facial recognition technology—across race, gender, and other demographic groups. The most significant takeaway from the NIST report is that it confirms current facial recognition technology performs far more effectively across racial and other demographic groups than had been widely reported; however, we've seen some misleading conclusions drawn from the highly technical 1,500-page report. A closer look at the findings in their proper context is essential to understanding the implications.

KEY TAKEAWAYS

- Facial recognition technology performs far more effectively across racial and other demographic groups than widely reported.
- The most accurate technologies displayed "undetectable" differences between demographic groups, calling into question claims of inherent bias.
- Key U.S. Government programs are using the most accurate technologies.
- Accuracy rates should always be considered in application-specific contexts.

ROLE OF NIST IN FACIAL RECOGNITION EVALUATION

For the past 20 years, NIST's Face Recognition Vendor Test (FRVT) program has been the world's most respected evaluator of facial recognition algorithms—examining technologies voluntarily provided by developers for independent testing. NIST's December report is the most comprehensive scientific evaluation to date of client facial recognition technology performance across demographic variables, involving 189 algorithms from 99 developers using 18 million images of 8 million people within 4 different data sets. The results are a snapshot in time, providing a critical benchmark against which developers work to improve the technology, as industry progress is tracked through the on-going FRVT program.

Purpose of the Report and What it Found

NIST's report addresses "assertions that demographic dependencies could lead to accuracy variations and potential bias"[2] as well as flaws in prior research and media reporting. "Much of the discussion of face recognition bias in recent years cites two studies showing poor accuracy of face gender classification algorithms on black women. Those studies did not evaluate face recognition algorithms, yet the results have been widely cited to indict their accuracy," according to the report.[3] The most-cited figure from those papers is that 2 such algorithms assigned the wrong gender to photos from that demographic group nearly 35 percent of the time. This was reported widely in media reports as a groundbreaking discovery on facial recognition accuracy even though it did not even assess this technology.

In contrast, NIST found that, "To the extent there are demographic differentials, they are much smaller," pointing out error rates in verification-type algorithms are "absolutely low," generally below 1 percent and many below 0.5 percent.[4] Even more significantly, NIST found that in the most accurate algorithms it tested, differences in performance across demographic groups were "undetectable." It would not be possible to mitigate these effects if bias is inherent in facial recognition technology, as some have alleged.

Notably for policy makers, the most well-known U.S. Government applications already use some of the highest-performing technologies. The report specifically identifies 6 suppliers of identification-type algorithms with undetectable differences in "false positive" rates.[5] Included among these are current technology suppliers to the

[1] Patrick Grether, Mei Ngan, and Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (Washington, DC: National Institute of Standards and Technology, December 2019), *https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf#page=69*.

[2] See Demographic Effects, pg. 1.

[3] See Demographic Effects, pg. 4.

[4] See Demographic Effects, pg. 54.

[5] See Demographic Effects, pg. 8.

Federal Bureau of Investigation Criminal Justice Information Services Division and U.S. Customs and Border Protection's Traveler Verification Service.

For the rest of the algorithms, the report found that higher overall accuracy means smaller differences in performance across demographic groups. NIST did find relatively higher false positive effects for some groups in the majority of algorithms tested—depending on the specific metric, type of algorithm, chosen similarity score threshold and data set involved. However, as one recent analysis of the report noted "Algorithms can have different error rates for different demographics but still be highly accurate."[6]

NIST charts comparisons across demographic groupings on a logarithmic scale because this granularity allows us to better perceive relative differences between error rates produced by algorithms that may be highly accurate in absolute terms. According to NIST, "readers don't perceive differences in numbers near 100 percent well," due to the "high nineties effect where numbers close to 100 are perceived indifferently."[7]

As a result, some figures in the report appear large if considered only in relative terms. Using photos from over 24 countries in 7 distinct global regions, verification-type algorithms produced false match rates for photos of individuals originally from East Africa as much as "100 times greater than baseline." Although performance variations across demographic groups are important to continually assess and critically examine, outside of Somalia nearly all country-to-country comparisons across algorithms yielded false match rates of less than 1 percent[8] despite the magnitude of differences identified.

Similarly, only 4 out of 116 algoritluns tested using the U.S. Mugshot Identification Database had false match rates of more than 1 percent for any demographic: Male, female, black, white, Asian, or American Indian.[9] One example cited by NIST produced a 0.025 percent false match rate for black males and a 0.1 percent false match rate for black women.[10] Compared to the rate for white males, this is 10 times higher for black women and 2.5 times higher for black males; however, these error rates are at or below 1⁄10 of 1 percent.

Certainly, significant gaps were found between the very highest- and lowest-performing algorithms. NIST tests any algorithm submitted and many of these are in the early stages of development. Lower-performing technologies are less likely to be deployed in commercial products.

ACCURACY IN CONTEXT

There will always be error rates for any biometric, or any technology for that matter. For example, this is why NIST compared false match rates for different demographic groups to each other, not zero. How is accuracy defined when it comes to demographic effects? According to NIST, it means these rates "do not vary (much) over any demographics."[11]

Overall, modern facial recognition technology is highly accurate. It is in fact image quality variations like pose, illumination, and expression have been the primary driver of errors in facial recognition performance, not demographic effects, and growing immunity to such problems is, according to NIST, the "fundamental reason why accuracy has improved since 2013."[12]

NIST has documented massive improvements in recent years, noting in 2018[13] the software tested was at least 20 times more accurate than it was in 2014, and in 2019[14] finding "close to perfect" performance by high-performing algorithms with

[6] Michael McLaughlin and Daniel Castro, "The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms are Neither Racist Nor Sexist," Information Technology and Innovation Foundation, Jan. 27, 2020, pg. 3, *https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms.*

[7] See Demographic Effects, pg. 22.

[8] See Demographic Effects, Annex 7.

[9] See Demographic Effects, Annex 6.

[10] See Demographic Effects, pg. 46, figure 12, imperial—002.

[11] See Demographic Effects, pg. 74.

[12] Patrick Grother, Mei Ngan and Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 2: Identification (Washington, DC: National Institute of Standards and Technology, September 2019), pg. 8, *https://www.nist.gov/system/files/documents/2019/09/11/nistir__8271__-20190911.pdf.*

[13] NIST Evaluation Shows Advance in Face Recognition Software's Capabilities, (Washington, DC: National Institute of Standards and Technology, November 2018), *https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities.*

[14] Patrick Grother, Mei Ngan, and Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 2: Identification (Washington, DC: National Institute of Standards and Technology, Sep-

miss rates averaging 0.1 percent. On this measurement, the accuracy of facial recognition is reaching that of automated fingerprint comparison, which is generally viewed as the gold standard for identification.[15]

LAB TESTS VS. REAL-WORLD

We simply aren't seeing instances in the United States where demographic performance differences in widely-used algorithms are affecting facial recognition systems in high-risk settings. There are several reasons that may explain why.

Algorithms comprise just one of several components of facial recognition systems. A human analyst will play a critical role in use of facial recognition as a tool in law enforcement investigations or as part of any process with potential high-consequence outcomes for individuals. There are no automated decisions made solely by the technology in these cases. Personnel adjudicates in situations where the technology may not work as well as intended. NIST has documented that the most accurate identification results occur when facial recognition is combined with trained human review, versus either element alone.[16] This may explain U.S. law enforcement's decade-plus operating history without any example of it contributing to a mistaken arrest or imprisonment.

False positives are naturally limited by the size of the data set used. A larger set of photos likely has a larger number of similar people in it; however, for many applications, the data sets are relatively small—the 250 passengers on a flight or 2 dozen people authorized to enter a building, for example, which will naturally limit false positives.

NIST calls for considering different accuracy measurements within the context of the "performance metric of interest" for specific applications, noting the study is the first to "properly report and distinguish between false positive and false negative effects."[17] The real-world implications of each depend entirely upon the specific use and mitigating factors. An error could be mostly inconsequential in cases where a "subject experiencing a false rejection could make a second attempt at recognition"[18] in order to unlock a door or device or clear passport control, for example.

One of the report's key findings was that false positive rates vary much more across demographic groups than false negative effects; however, false negative effects are more critical to many uses identified.[19] For example, facial recognition is used to detect fraud attempts when the same person applies for driver's license applications under different identities, ensuring this person is not the same as any other in a database. This is also how it works in many security applications, where the purpose of photo comparison is to ensure persons entering a building do not match those on a persons of interest list. In both cases, the false negative rate is the key performance measurement because the antifraud or security objective requires a very low likelihood of missing a possible match to flag for human review.

For law enforcement investigations, ensuring that possible matches are not missed is even more critical. According to the NIST report, "false positive differentials from the algorithm are immaterial" for law enforcement investigations since all searches produce a fixed number of candidates for human review regardless of any threshold for similarity score.[20] On the other hand, at a port of entry, there may be a relatively high risk of persons attempting to enter under another identity, so false positive effects may be more critical. In a low-risk application like entry to an amusement park, both accuracy measurements may be less critical due to the low probability of someone trying to impersonate someone with a ticket and the operational need to speed entry by limiting rejections.

LIMITATIONS OF THE REPORT

Despite taking the most comprehensive look so far at demographic effects in facial recognition performance, the NIST report does have limitations and raises some unanswered questions. Most significantly, it is not clear whether ethnicity was fully

tember 2019), pg. 6, *https://www.nist.gov/system/files/documents/2019/09/11/nistir__8271-__20190911.pdf.*

[15] See NIST's most recent fingerprint vendor technology evaluation of the most accurate submissions for ten finger (rolled-to-rolled) samples, *https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8034.pdf.*

[16] NIST Study Shows Face Recognition Experts Perform Better With AI as Partner, (Washington, DC: National Institute of Standards and Technology, May 2018), *https://www.nist.gov/news-events/news/2018/05/nist-study-shows-face-recognition-experts-perform-better-ai-partner*.

[17] See Demographic Effects. pg. 18.

[18] See Demographic Effects, pg. 58.

[19] See Demographic Effects, charts on pgs. 29, 62.

[20] See Demographic Effects, pg. 5.

isolated from other demographics or capture conditions in many instances. For example, false match rates for Somalia are very significant outliers that are not fully explained. These error rates are far higher for Somalians than neighboring countries in nearly every algorithm tested. For example, one of the most accurate verification algorithms overall had a false match rate of about 1 percent for Somalia, while for neighboring Ethiopia—which has a closely related ethnic majority—it was just 0.07 percent, more than 14 times lower.[21] This dramatic difference would suggest that the impact of ethnicity was not isolated and that other differences, in capture conditions, data labeling errors, etc. between country data exist.

IMPLICATIONS FOR THE SECURITY INDUSTRY

Applied to security solutions developed by our industry, biometric technologies like facial recognition increase the effectiveness of safety and security measures that protect people from harm. Any significant bias in technology performance makes it harder to achieve this goal.

We understand that there are legitimate concerns that use of facial recognition technology might negatively impact women and minorities. Industry is striving to provide technology that is as effective and accurate as possible across all types of uses, deployment settings and demographic characteristics in order to fully address these concerns.

Both developers and end-users have a responsibility to minimize any negative effects that could result when the technology does not perform as intended though proper design, configuration, policies, and procedures. We strongly believe that facial recognition makes our country safer and brings value to our everyday lives when used effectively and responsibly. No technology product should ever be used for purposes that are unlawful, unethical, or discriminatory.

FACE FACTS: HOW FACIAL RECOGNITION MAKES US SAFER & THE DANGERS OF A BLANKET BAN

Facial recognition technology makes our country safer and brings value to our everyday lives when used effectively and responsibly. The Security Industry Association (SIA) believes all technology products, including facial recognition technology, must only be used for purposes that are lawful, ethical, and nondiscriminatory.

- Modern facial recognition technology is highly accurate. The National Institute of Standards and Technology (NIST) found that the facial recognition software it tests is now over 20 times better than it was in 2014 at searching a database to find a matching photograph. NIST's September 2019 report found "close to perfect" performance by high-performing algorithms with miss rates averaging 0.1 percent, reaching the accuracy of fingerprint comparison technology—the gold standard for identification.
- The benefits of facial recognition have been proven for more than a decade of use in real-world applications, including finding missing and exploited children, protecting critical infrastructure, and aiding law enforcement investigations. See examples of the benefits in action on the reverse page.

WHY A BLANKET BAN PUTS AMERICANS AT RISK

- A blanket ban on Government use precludes all possible current and future applications of the technology, regardless of the purpose, putting the safety of every resident at risk.
- Beyond law enforcement, such a ban prohibits other proven uses like secured employee access to critical infrastructure and other systems that protect building occupants and software that detects fraud against Government programs, to name a few.
- Such bans have also been defined broadly, prohibiting any Government official, employee, contractor or vendor from using any technology with facial recognition capabilities, including social media platforms and smartphones.
- A ban on facial recognition eliminates a useful tool that is being used alongside human intelligence. Thorough analysis must acknowledge the alternatives a ban would leave us with—far slower and less accurate identification processes chat are much more prone to errors (for example, detectives sifting manually through hundreds or even thousands of videos and images of arrested individuals based on suspect descriptions). NIST confirmed in a 2018 study chat the highest identification accuracy is achieved through human analysis supported by facial recognition technology versus either element alone.

[21] See Demographic Effects, Annex 7, pg. 226, tevian–005.

- Before taking such an extreme step, policy makers must thoroughly examine how the technology is used and consider all the options available to address concerns. Sensible transparency and accountability measures can be identified that would ensure responsible use of the technology without unreasonably restricting cools chat have become so essential to public safety.

FACE FACTS: KEEPING AMERICANS SAFE

SAVING SEX TRAFFICKING VICTIMS.—In April 2019, a California law enforcement officer saw a social media post about a missing child from the National Center for Missing and Exploited Children. The officer used facial recognition which returned a list of on-line sex ads featuring the girl.

According to a story in WIRED, the girl had been "sold for weeks," and the officer's actions helped a process that "recovered and removed from the girl from trauma."

CATCHING A NEW YORK CITY SUBWAY TERRORIST.—In August 2019, New York Police Department detectives used facial recognition to help identify a man who sparked terror by leaving rice cookers in and around a subway station. Detectives pulled still images from security footage and used facial recognition software, along with additional investigative work, to identify the suspect within an hour: NYPD officials were quoted saying, "To not use technology like this would be negligent" and "This is the most important type of case that we'd see out there: a possible terrorist attack in NYC."

FINDING A KILLER WHO TARGETED LGBTQ VICTIMS.—On May 25, 2019, in Wayne County, Michigan, 3 members of the LGBTQ community were shot and killed by a man at a gas station. The Detroit Police Department used facial recognition, as well as their own intelligence, to help identify the suspect, who was charged with 3 counts of murder in addition to other charges.

IDENTIFYING THE CAPITAL GAZETTE KILLER.—Jarrod Ramos was angered by a story the *Capital Gazette Newspaper* in Annapolis, Maryland, ran about him in 2011 and brought a lawsuit against the paper for defamation, which a judge later dismissed. In June 2018, Ramos entered the newspaper building with a shotgun and killed 5 employees, leaving 2 others critically injured. Anne Arundel Police obtained an image of Ramos and sent it to the Maryland Combined Analysis Center, which helped identify him by comparing the photo to others in the Maryland Image Repository System.

APPREHENDING PEDOPHILES EVADING JUSTICE.—In 2017, after a 16-year manhunt, a man accused of sexually assaulting a minor was apprehended in Oregon. Using facial recognition technology, the Federal Bureau of Investigation (FBI) was able to identify the suspect after a positive match was found when the suspect sought to acquire a U.S. passport. Similarly, in 2014, the FBI used facial recognition technology to help locate and apprehend a convicted pedophile who had been on the run for 14 years.

PREVENTING ENTRY INTO THE UNITED STATES UNDER FALSE IDENTITIES.—After just 3 days of operation, facial recognition technology at Dulles International Airport in Virginia caught a man trying to use a fake passport to enter the United States. The fraudulent passport would have easily gone undetected with visual inspection alone. The ability to enter under a false identity is essential to organized crime, human trafficking, money laundering, drug smuggling, terrorism, and many other criminal activities. According to U.S. Customs & Border Protection, use of the technology prevented 26 alleged imposters from entering the United States in just a 3-month span in 2018.

Article From the Information Technology and Innovation Foundation (ITIF)

The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist

By: Michael McLaughlin and Daniel Castro / January 2020

A close look at data from a new NIST report reveals that the best facial recognition algorithms in the world are highly accurate and have vanishingly small differences in their rates of false positive or false-negative readings across demographic groups.

INTRODUCTION

The National Institute of Standards and Technology (NIST) recently released a report that examined the accuracy of facial recognition algorithms across different demographic groups. The NIST report found that the most accurate algorithms were highly accurate across all demographic groups. But NIST tested nearly 200 algorithms from vendors and labs around the world—it allows anyone to submit an algorithm for testing—and since many of the algorithms it tested displayed some bias, several news outlets and activists have misleadingly concluded that facial recognition systems are racist and sexist.[1] But a close look at the data reveals a different picture.

Facial recognition technology compares images of faces to determine their similarity, which the technology represents using a similarity score. The technology often performs one of two types of comparisons. The first comparison is known as a one-to-many or identification search, in which the technology uses a probe image to search a database of images to find potential matches. The second comparison is known as a one-to-one or verification search as the technology compares 2 images to determine the similarity of the faces in them. In many cases, the faces in images are considered a match if their similarity score meets or exceeds the match threshold, a number the operator assigns that represents a minimum acceptable similarity score. The technology has many commercial and non-commercial uses, and will likely be integrated into more products and services in the future to enhance security, improve convenience, and increase efficiency. such as by helping find victims of human trafficking. expediting passengers through airport security, and flagging individuals using forged identification.[2]

NIST assessed the false positive and false-negative rates of algorithms using 4 types of images, including mugshots, application photographs from individuals applying for immigration benefits, visa photographs, and images taken of travelers entering the United States. NIST's report reveals that:

- The most accurate identification algorithms have " undetectable" differences between demographic groups;[3]
- The most accurate verification algorithms have low false positives and false negatives across most demographic groups;[4]
- Algorithms can have different error rates for different demographics but still be highly accurate.

KEY FINDINGS

As detailed below, NIST found that the most accurate algorithms—which should be the only algorithms used in Government systems—did not display a significant demographic bias. For example, 17 of the highest-performing verification algorithms had similar levels of accuracy for black females and white males: False-negative rates of 0.49 percent or less for black females (equivalent to an error rate of less than 1 in 200) and 0.85 percent or less for white males (equivalent to an error rate of less than 1.7 in 200).[5]

[1] Tom Higgins "'Racist and Sexist' Facial Recognition Cameras Could Lead to False Arrests," *The Telegraph,* December 20, 2019, *https://www.telegraph.co.uk/technology/2019/12/20/racist-sexist-facial-recognition-cameras-could-lead-false-arrests.*

[2] Tom Simonite, "How Facial Recognition Is Fighting Child Sex Trafficking," *Wired,* June 19 2019, *https://www.wired.com/story/how-facial-recognition-fighting-child-sex-trafficking/;* "Face Recognition Nabs Fake Passport User at US Airport," *VOA News,* August 24, 2018 *https://www.voanews.com/silicon-valley-technology/face-recognition-nabs-fake-passport-user-us-airport.*

[3] We defined the most accurate identification algorithms as the 20 algorithms that had the lowest false-negative identification rates for placing the correct individual at rank one when searching a database that had images of 12 million individuals in NIST's September 2019 identification report. NIST provided error characteristics data by race and sex for 10 of these algorithms in its recent report. Consequently, we analyzed the performance of NEC–2, NEC–3, Visionlabs–7 , Microsoft–5, Yitu–5, Microsoft–0, Cogent–3, ISystems–3, NeuroTechnology–5, and NTechlab–6; Patrick Grother, Mei Ngan, and Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 2: Identification (Washington, DC: National Institute of Standards and Technology, September 2019), 47 *https://www.nist.gov/system/files/documents/2019/09/11/nistir_8271_20190911.pdf#page=49.*

[4] We defined the most accurate verification algorithms as those that rank in the top 20 on NIST's FRVT 1:1 leaderboard on January 6, 2020. NIST has since updated the leaderboard. Not all of these algorithms were tested in NIST's most recent demographics report. We analyzed the performance of algorithms that NIST provided data for in Annexes 6, 13, 15, and Figure 22. These algorithms are visionlabs–007, everai-paravision–003, didiglobalface–001, imperial–002, dahua–003, tevian–005, alphaface–001, ntechlab–007, yitu–003, innovatrics–006, facesoft–000, intellifusion–001, anke–004, hik–001, camvi–004, vocord–007, and tech5–003; National Institute of Standards and Technology, FRVT 1:1 Verification (FRVT 1: 1 leaderboard, accessed January 6, 2020), *https://pages.nist.gov/frvt/html/frvt11.html.*

[5] The high-performing algorithms include visionlabs–007, everai-paravision–003, didiglobalface–001, imperial–002, dahua–003, tevian–005, alphaface–001, ntechlab–007, yitu–003, innovatrics–006, facesoft–000, intellifusion–001, anke–004, hik–001, camvi–004, vocord–007, and tech5–003. Comparisons made at the same match threshold.

While the most accurate algorithms did not display a significant demographic bias, it is also true that the majority of the algorithms NIST tested generally performed better on men and individuals with lighter skin tones. However, it is important to recognize that there is a stark difference between the best and worst algorithms. In comparison to the false-negative rates under 1 percent for black females and white males among the highest-performing algorithms, the lowest-performing algorithms had false-negatives rates, for blacks and whites, as high as 99 percent.[6] This wide range of accuracy is not surprising considering that NIST allows anyone to submit an algorithm for testing, ranging from large companies with production systems to small research groups whose algorithms have not left the lab—algorithms are tested even if they are not incorporated into a commercially-available product.

The Most Accurate Identification Algorithms Have Undetectable Differences Between Demographics

NIST found that some highly-accurate algorithms had false-positive demographic differentials that were so small as to be "undetectable" for one-to-many searches.[7] Moreover, for most algorithms, black men had lower false-negative rates than white men, and several of the top algorithms had better false-negative rates for white women than white men.[8] Several algorithms also provided uniform similarity scores across demographic groups, meaning that the algorithms provided similar match and non-match scores regardless of race and gender.[9] The uniform scores indicate that these algorithms would have small demographic differentials if an operator applied a threshold. But different thresholds can affect demographic differentials. For example, at least 6 of the most accurate identification algorithms had higher false-positive rates for black men than white men at one threshold, but lower false-positive rates for black men than white men at another threshold.[10]

The Most Accurate Verification Algorithms Have Low False Positives and Negatives Across Most Demographics

The most accurate verification algorithms have low false positives and negatives across most demographics. For example, when NIST applied thresholds so that the algorithms had false positive rates of 0.01 percent for white males, more than half of the 17 most accurate algorithms had false-positive rates of 0.03 percent or better for black males, Asian men, and white women.[11] This equates to the algorithms falsely matching these individuals 3 times or less per every 10,000 comparisons to an imposter compared to 1 per every 10,000 for white males. At another threshold, 7 of the top algorithms displayed no false-positive bias between white men, black men, Asian men, and white females.[12] At this threshold, several algorithms also had false-positive rates of 0.003 percent or less for black women or Asian women while white males had false-positive rates of 0.001 percent.[13]

[6] The low-performing algorithms, according to their performance for false non-match rate on Figure 22 of the NIST demographics report, include shaman–001, isap–001, ayonix–000, amplifiedgroup–001, saffe–001, videonetics–001, and chtface–001.

[7] Patrick Grether, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (Washington, DC: National Institute of Standards and Technology, December 2019), 3, *https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf#page=6.*

[8] To compare white men and white women, we analyzed false-negative rates for ranking the correct matching image as the top potential match. Algorithms that had lower false-negative rates for white women than white men include NEC–2, NEC–3, and Visionlabs–7; Patrick Grether, Mei Ngan, and Kayee Hanaoka, Face Recognition Vendor Test(FRVT) Part 3: Demographic Effects (Washington, DC: National Institute of Standards and Technology, December 2019), 63 *https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf#page=66;* National Institute of Standards and Technology, On-going Face Recognition Vendor Test (FRVT) (part 3: demographic effects, annex 16: identification error characteristics by race and sex), *https://pages.nist.gov/frvt/reports/demographics/annexes/annex_16.pdf.*

[9] Patrick Grether, Mei Ngan, and Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (Washington, DC: National Institute of Standards and Technology, December 2019), 66, *https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf#page=69.*

[10] These algorithms include Visionlabs–7, Microsoft–5, Yitu–5, Microsoft–0, ISystems–3, and NeuroTechnology–5; National Institute of Standards and Technology, On-going Face Recognition Vendor Test (FRVT) (part 3: demographic effects, annex 16: identification error characteristics by race and sex), *https://pages.nist.gov/frvt/reports/demographics/annexes/annex_16.pdf.*

[11] One of these algorithms, for example, is visionlabs–007; National Institute of Standards and Technology, On-going Face Recognition Vendor Test (FRVT) (part 3: demographic effects, annex 6: cross-race and sex false match rates in United States mugshot images), *https://pages.nist.gov/frvt/reports/demographics/annexes/annex_06.pdf.*

[12] An example of such an algorithm is anke–004.

[13] An example of such an algorithm is yitu–003.

False negatives were also low for the most accurate verification algorithms. Five of the 17 most accurate algorithms had false-negative rates of less than 1 percent across all demographic groups when NIST applied a threshold that set false-positive rates at 0.01 percent.[14] Similarly, the best verification algorithms had less than 1 percent false-negative rates across countries and demographic groups. For example, the algorithm Visionlabs–007 had below a 1 percent false-negative rate for nearly all countries and demographic groups for border crossing application images. There were two exceptions—Somalian and Liberian women under 45. Nonetheless, the algorithm had a false-negative rate below 1.4 percent for each of these groups.

Algorithms Can Have Different Error Rates for Different Demographics But Still Be Highly Accurate

Some algorithms perform differently on one group compared to another, but still maintain true positive and true negative accuracy rates greater than 99 percent for all races and sexes.[15] Because these algorithms have very low error rates, differences that are small in absolute terms may seem large if expressed in relative terms. For example, an algorithm from Dutch firm VisionLabs, Visionlabs–007, had a false-negative rate 4 times higher for the nationality it performed poorest on (Somalian) than the nationality it performed best on (Salvadoran).[16] Nonetheless, the algorithm only had a false-negative rate of 0.63 percent for individuals from Somalia. Another example is the performance difference of a verification algorithm from Camvi, a firm based in Silicon Valley, for white males and American Indian females. At one particular threshold, the algorithm had a false-positive rate that was 13 times higher for American Indian females than white men.[17] But at this threshold, the algorithm had barely more than 1 false match of American Indian females for every 10,000 imposter comparisons to other American Indian females. It is also true that most verification algorithms had higher false-negative rates for women than men. But NIST notes that this "is a marginal effect—perhaps 98 percent of women are still correctly verified—so the effect is confined to fewer than 2 percent of comparisons where algorithms fail to verify."

PUTTING NIST'S DATA IN CONTEXT

Recent reporting on how law enforcement in San Diego used facial recognition from 2012–2019 can also help put NIST's data in context. In 2018, various law enforcement entities made 25,102 queries to a database of 1.8 million mugshot images.[18] Law enforcement officials uses of the technology included attempts to determine whether an individual had a criminal record and attempts to discover the identity of individuals who lacked identification. These use cases were likely one-to-many searches. Law enforcement did not track the success of the program, making it unclear how many false positives or false negatives the system registered as well as how many mated or non-mated searches—a search in which an image of the individual was not in San Diego's database—they performed.

But we can consider a few scenarios to make a rough estimate of how the most accurate algorithms might perform in a city like San Diego, assuming San Diego's images and hardware were of similar quality to NIST's.[19] Under the first scenario, let us assume that all 25,102 probe images law enforcement used had a match in the database of 1.8 million mugshot images (an unlikely event), and that law enforcement did not apply a threshold to limit false positives or negatives (also unlikely). NEC–2, the best identification algorithm NIST tested in an earlier 2019 report, failed to rank the correct candidate as the most likely match only 0.12 percent of the time when performing a search of a database containing images of 3 million

[14] These algorithms are visionlabs–007, everai-paravision–003, didiglobalface–001, alphaface 001, and intellifusion–001; National Institute of Standards and Technology, On-going Face Recognition Vendor Test (FRVT) (part 3: demographic effects, annex 15: genuine and imposter score distributions for United States mugshots), *https://pages.nist.gov/frvt/reports/demographics/annexes/an nex__15.pdf.*

[15] These algorithms include visionlabs–007 and everai-paravision–003.

[16] In this case, NIST set the threshold to "the lowest value that gives FMR less than or equal to 0.00001."

[17] National Institute of Standards and Technology, On-going Face Recognition Vendor Test (FRVT) (part 3: demographic effects, annex 15: genuine and imposter score distributions for United States mugshots, 19), *https://pages.nist.gov/frvt/reports/demographics/annexes/annex__15.pdf#20.*

[18] DJ Pangburn, "San Diego's Massive, 7-Year Experiment With Facial Recognition Technology Appears to Be a Flop," Fast Company, January 9, 2020, *https://www.fastcompany.com/90440198/san-diegos-massive-7-year-experiment-with-facial-recognition-technology-appears-to-be-a-flop.*

[19] In each of the scenarios, we are assuming that the racial and gender makeup of San Diego's mugshot database is similar to NIST's mugshot database.

individuals.[20] At this rate, the technology would have succeeded in listing the correct individual in the San Diego search as the most likely match 24,970 times out of the 25,000 searches and failed 30 times.

Under a second scenario, let us assume law enforcement applied a threshold that allowed for 1 false positive every 1,000 non-mate searches. At this rate, NEC–3 had a false-negative rate of 0.26 percent. We also assume that half of the more than 25,000 probe images had a match in the database and that half did not have a match. In this scenario, the algorithm would have registered 13 false positives and 33 false negatives.

CONCLUSION

Developers and users of facial recognition technology, law enforcement, and lawmakers can take several actions to promote the development and responsible use of facial recognition technology. First, developers should continue to improve accuracy rates across different demographics, including by diversifying their datasets.[21] Second, the Government should set standards for the accuracy rates of the systems it deploys. Third, law enforcement should have standards for the quality of images it uses in a facial recognition search, which can affect the accuracy of facial recognition algorithms.[22] Fourth, the users of facial recognition technology should carefully choose which match threshold is appropriate for their goal. Last, lawmakers should consider how law enforcement typically uses the technology and the different implications of false positive and false negatives when developing regulations. In most law enforcement scenarios, law enforcement is using facial recognition technology to return a list of possible suspects that humans review. And there are different implications when algorithms incur false positives or false negatives. In many cases, a subject can make a second attempt at recognition when a facial recognition system produces a false negative. This implication differs from the possible effects of false positives, which could allow an individual access to a facility they should not enter.

Finally, while there is no place for racial, gender, or other types of discrimination in societies, to ban facial recognition unless it performs exactly the same across every conceivable group is impractical and would limit the use of a societally valuable technology. Many critics of facial recognition technology complain that the technology is not accurate enough, but refuse to give specifics on what they would consider sufficient—refusing to set a clear goal post for industry—which suggests they are not serious about wanting to improve the technology and oppose it for other reasons.

Reasonable people may disagree on when it is appropriate to use facial recognition, but the facts are clear that the technology can be highly accurate. As previous NIST reports have shown, many of the algorithms have accuracy rates that exceed 99 percent, and as the new report shows, the differences across demographics are minimal for the best algorithms.[23]

Mr. ROGERS. Thank you, sir.

Chairman THOMPSON. The Chair recognizes the gentlelady from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Let me thank the Chairman very much.

Let me acknowledge all of the Government witnesses and thank them for their service.

[20] Patrick Grother, Mei Ngan, and Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 2: Identification (Washington, DC: National Institute of Standards and Technology, September 2019), 47, *https://www.nist.gov/system/files/documents/2019/09/11/nistir__8271__20190911.pdf#page=49.*

[21] Chinese developers often had lower false positives for Chinese faces, suggesting that increasing the representation of minority faces in training data may reduce bias.

[22] For example, although the false-negative rates were frequently lowest for black individuals in mugshot images, false-negative rates were relatively high for black individuals in images taken at border crossings. This difference could result from inadequate exposure in the latter photos; Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (Washington, DC: National Institute of Standards and Technology, December 2019), 54, *https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf#page=57.*

[23] For example, a previous NIST report revealed that the top 20 identification algorithms failed to place the correct individual as the top potential match when searching a database containing images of 12 million individuals less than 1 percent of the time; Patrick Grother, Mei Ngan, and Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 2:—Identification (Washington, DC: National Institute of Standards and Technology, September 2019), 47, *https://www.nist.gov/system/files/documents/2019/09/11/nistir__8271__20190911.pdf#page=49.*

Let me renew the inquiry that will be pursued by Chairwoman Rice, but I will add to it, and that is, Mr. Wagner, a better understanding. Maybe you will provide the information to the committee on the denial of clear global and Trusted Traveler as relates to States that may not have the laws that you think are appropriate or, in the instance of New York, closing out access to the issue of driver's license.

I raise the question because we should look as the Federal Government at what other identification options may be valid.

I know that we have known each other for a long time, and I would think that you would be willing to look at that so that we can find common ground.

Let me pursue this line of reasoning, and please, witnesses, understand that I am not saying this is what you are doing. I need to understand your thinking.

So to the Deputy Executive Assistant Commissioner Wagner, would you accept the fact that bias could be introduced by technology if the application developer of the program had a bias into how an application reacts to different types of people because it is technology?

Mr. WAGNER. Yes.

Ms. JACKSON LEE. I would also make the point though it is a little bit humorous, is I am sure the people in Iowa were trusting of the app and thought they had something going on there, and we all can see where we are at this point.

Would you accept that, Mr. Mina?

Mr. MINA. Yes, Congresswoman.

Ms. JACKSON LEE. Would NIST accept that, Mr. Romine?

Mr. ROMINE. Yes.

Ms. JACKSON LEE. Yes. An algorithm could be—again, know that this is not pointed toward you—be written to flag all black males wearing dreadlocks.

Mr. Wagner, this is in terms of how technology can be.

Mr. WAGNER. I guess you could.

Ms. JACKSON LEE. I understand. You can say on the record to your knowledge, you are not using that kind of algorithm.

Mr. WAGNER. We are not using that. I can——

Ms. JACKSON LEE. That would be very good. I am sure dreadlock wearers would be glad of that.

Mr. Mina.

Mr. MINA. Yes, that is possible, and again, as Mr. Wagner said, we have not seen that in our review as well.

Ms. JACKSON LEE. All right. Mr. Romine.

Mr. ROMINE. It is certainly possible.

Ms. JACKSON LEE. OK. So here we are. Let me to my colleagues over here that are DNA advocates, as a member of the Judiciary Committee, which I had to step away from, we are DNA lovers. I wrote the Violence Against Women Act and put in $291 million for DNA enhancement. So we understand that as the new added technology.

But as the Department of Homeland Security, we made a commitment post-9/11 with George Bush going to the Trade and saying he heard the firefighters, but at the same time he also heard Muslims who were indicating it is not the blanket world of people who happen to be Muslim.

So, in particular, Mr. Mina, I want to try to find out what aggressive role do you play in helping to not have platitudes. Forgive me. I am not suggesting you do, but to aggressively ensure that the biases against black women with dreadlocks, men with dreadlocks, Muslims or Sikhs wearing attire.

I went through that. I have been on this committee since its beginning. That is not technology, but and then now sophisticated technology is not undermining the civil liberties and civil rights of this Nation and those coming in innocently to the country. You can use the new technology as well.

Then to Mr. Romine, let me find out how are you continuing to do your assessment of these algorithms to ensure that it looks like you were not able to get the exact one that Mr. Wagner's team is using. That concerns me.

I need you to get every accurate piece of information, and I would like you to say that.

Mr. Mina, what aggressiveness are you doing to protect the travelers and the American people?

Mr. MINA. I thank you for the question, Congresswoman.

So I think we are doing a lot of different things across the spectrum and the life cycle of this program and policy, and again, I want to focus. Our attention is really on the application, not so much on the algorithm itself, but on how it is applied by particularly a DHS program, in this case, CBP.

We do that through, on the policy-making side, working directly with the component, advising on proposed regulations of implementing policies, as well as offering suggestions as it relates to applications, for example, folks wearing religious headwear or folks that have objections to photography based on religious reasons or the people who are disabled or otherwise injured and area not able to take pictures.

We also do it through our robust community engagement. We talk to members of the community across the country, and, Mr. Chairman, I actually have the information in front of me regarding some of the areas.

It is the issues that have been raised in Portland, in Atlanta, in Chicago and Seattle, and then also to a lesser extent in Southern California, primarily L.A. and Orange County, and then by New York City area stakeholders where we have heard concerns regarding facial recognition technology.

One of our primary roles is to be the eyes and ears of the Department, and we inform our colleagues at CBP, at DHS S&T, at OBIM. Here are the concerns that we are seeing. How do we work together to try and address some of these problems or potential problems before they have even greater effect?

Then also, on the back end we have a robust compliance process, and while we do not have an active investigation right now on facial recognition, that is always something that we are looking at. If we see a trend, we will most certainly open an investigation and, again, advice in that way as well.

Ms. JACKSON LEE. Would you be kind enough, Mr. Chairman, to let Mr. Romine answer his question?

As he answers, Mr. Chairman, I just want to say this on the record, if we can get answers from Mr. Wagner about what is stored in terms of retaining information.

Chairman THOMPSON. Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you. Mr.——

Chairman THOMPSON. No. Dr. Romine, you can answer the question. You can submit in writing to Ms. Jackson Lee.

Ms. JACKSON LEE. No, that is what I am saying.

Chairman THOMPSON. Yes.

Ms. JACKSON LEE. Yes. Thank you.

Chairman THOMPSON. Be happy to do it.

Ms. JACKSON LEE. Thank you.

Mr. Romine, my question was——

Mr. ROMINE. I beg your pardon, ma'am?

Ms. JACKSON LEE. Yes. My question was: What are you doing to be accurate in your testing?

You said you did not know whether you had the accurate app that they were using. What are you doing to be aggressive in making sure that we do not have the bias in these algorithms?

Mr. ROMINE. Yes, ma'am. The tests that we undertake are intended to determine whether there are demographic differences, commonly called bias. The fact that I know there is strong interest in testing with data that is more representative, and we have signed a recent MOU with the CBP to undertake continued testing to make sure that we are doing the very best that we can to provide the information that they need to make sound decisions.

Ms. JACKSON LEE. Thank you very much.

I yield back. Thank you.

Chairman THOMPSON. Thank you.

The Chair recognizes the gentleman from Texas, Mr. Green.

Mr. GREEN of Texas. Thank you, Mr. Chairman.

I thank the witnesses for appearing as well.

I would like to address some intelligence that has been afforded me. The indication is that NIST found that Asian and African American faces were 10 times more likely, well, 10 to 100 times more likely to be misidentified than white faces.

I am curious as to whether or not there is something inherent in the technology that creates an inverse relationship with reference to the identification of whites juxtaposed to African Americans and Asians.

Is there something inherent in the technology, meaning if you want to absolutely identify whites, will there be something that you cannot adjust such that you will get the same absolute identification with minorities, Asians, African Americans?

Or if you want to absolutely identify African Americans and Asians, will you, as a result of technology, not be able to properly identify whites?

Mr. ROMINE. It is a very interesting question, Congressman.

Mr. GREEN of Texas. Thank you.

Mr. ROMINE. Let me clarify first that those differentials that we observed were not in the case of identification but rather verification, the one-to-one testing rather than the one-to-many testing. In general, we saw those demographic differences for African Americans and for Pacific Islanders and Asians as well.

But in the case that you are talking about, our work has not to-date focused on cause and effect. What is it that is causing the algorithms to exhibit certain kinds of behavior? We are really just testing the performance.

So I do not know the answer to your question.

Mr. GREEN of Texas. My question was interesting, as you put it. Your answer is intriguing because this is not the first opportunity for the word to be heard that we have these difficulties, and at some point, it would seem that we would move from testing technology as it is to understanding why technology performs the way it does.

Help me to understand why we have not made that move?

Mr. ROMINE. The question that you asked is a very challenging open research question, but we do have some indications.

There are algorithms that have been submitted to our testing from Asian countries that do not exhibit the demographic differentials on Asian faces. So we cannot guarantee, but we think that is an indication that the training data that are being used for the algorithm development may have a significant impact on their ability to discern or exhibit demographic differences for different populations.

Mr. GREEN of Texas. Do you believe that it is important for us to move expeditiously to answer this question, to resolve this issue such that we do not find ourselves having deployed something en masse that we know to be defective or have some degree of inefficiencies associated with it?

The efficacy of this is important.

Mr. ROMINE. Yes, sir, and I think those are two different things to think about. The performance testing that we currently execute can help operational agencies ensure that they are not deploying things that exhibit demographic differentials.

The research question that you teed up that is fascinating about what are the causes of these demographic differentials is a much deeper question and much more difficult, I think.

Mr. GREEN of Texas. Well, is it fair to say that the countries—and I have about 45 seconds left—but the countries that employ the technology that have indicated to you they are having fewer challenges, is it fair to say that that technology also captures white men sufficiently?

Mr. ROMINE. In the testing that we did for the specific one that I am referring to, the high-performing algorithms from Asian countries that do not exhibit the demographic differences on Asians, it is in comparison to Caucasian faces that I made that statement.

So there is no difference in the performance or discernable difference in the performance on Caucasian faces and Asian faces from certain Asian-developed algorithms, and one speculation is that it may be the training data that are used.

Mr. GREEN of Texas. Thank you, Mr. Chairman. I yield back.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the gentleman from Rhode Island for 5 minutes. Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

I want to thank our witnesses for your testimony here today, and thank you for you are doing, your dedication to this issue, a very important issue.

I certainly believe that technology is an important part of the solutions that some of our most vexing issues and challenges, including how to manage an ever-growing number of international travelers. So it has been a good discussion here today.

What I wanted to ask of either Mr. Wagner or Mr. Mina, we know that in technological solutions, such as facial recognition software, the algorithms are only as good as the data that inform them. So I want to know how has CBP adjusted or augmented the data that it uses to train its facial recognition software.

What are you doing to ensure the software is continually updated as more robust data sets and algorithms are incorporated into training?

Mr. WAGNER. That is where we work closely with the vendor, whose algorithm we are using, NEC, and we work closely with them to incorporate their updates and their latest and greatest products into how we are using them.

Then as we review the data, you know, we look to make those operational adjustments, which do impact metrics, and again, that is going to be the quality of the photograph, the quality of the camera, the human factors.

The size of the gallery is really important, and you know, in this, it tested galleries up to, I think, 12 million people. You know, on the margins of the capabilities of these algorithms, we are doing this on a couple thousand, and interesting correlations are how much better improved is your match rates and what is the impact on any potential demographic biases on a much smaller gallery or sample size.

I think that is what we were getting at earlier, that what are these variables that we can raise or lower to help address some of what the error rates are showing us.

Mr. LANGEVIN. OK. So to that point then, how does CBP incorporate feedback from officers about errors that facial recognition software has made in the field?

Because the machine, it learns. When the officer is looking, interacting with someone, and the software does not get it correct, unless that feedback is fed back into the system, the system does not learn.

Mr. WAGNER. Oh, absolutely, and that is where we look at the system logs themselves, but we also talk to the officers. They provide the feedback, and then we are also on-site to witness and observe and discuss with those officers as we deploy these.

Mr. LANGEVIN. That is important.

So I understand the Trusted Traveler Program shares information with other countries, and how does CBP share biometric information with other countries and what steps does it take to ensure that those countries use the data responsibly?

Is that accurate, No. 1, what my understanding is?

How are we guarding that data to make sure that they are protected it?

Mr. WAGNER. I am trying to think of when. I am not aware of how we would share or if we are even sharing.

Mr. LANGEVIN. With the Trusted Traveler Program.

Mr. WAGNER. We do not share. We might share a person's status that they are approved in the program, but we are not actually sharing, say, their fingerprints.

Mr. LANGEVIN. OK. So let me ask that one for the record, and I would ask that you get back to me on that.

Mr. WAGNER. Yes.

Mr. LANGEVIN. This is important.

What types of information do we share under the Trusted Traveler Program? I think that is important for us to know.

If we do share, whatever information we share, I want to know what steps we take to ensure that those countries use that data responsibly.

So I know that this question has been touched on earlier. So I am going to ask it perhaps in a different way, but just prior to our hearing on this topic, last July we were notified of a cyber incident on the network of a CBP subcontractor. Someone claiming to be a foreign agent gained access to tens of thousands of photos of driver's faces and license plates at a port of entry along the Southern Border.

How is CBP ensuring that the personal data it collects for facial recognition technology screening programs, whether by the Government directly or by vendors or their private-sector partners, are being protected from inadvertent or otherwise unauthorized access?

Also, what assurances can you give our committee that the root causes of the May 2019 breach have been addressed so as to reduce the likelihood of another breach?

Mr. WAGNER. So the airlines and airports that provide the cameras that take the pictures to transmit them to CBP, we have a signed set of business requirements with them which they commit to not storing, not sharing, not saving any of the photographs that they take.

They take the picture, have to transmit it to us, and purge it from their system.

One of the other conditions is that they have to be available for CBP to audit their cameras and their technology to ensure that they are following those rules.

We are about to commence an audit on one of the airlines in the next couple of months and start that process to do that, but to make sure that that is not happening.

Mr. LANGEVIN. Thank you.

Mr. Chairman, I would ask that Mr. Wagner get back with me in writing as soon as possible on that Trusted Traveler Program and what information is shared with partners.

Chairman THOMPSON. OK.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you.

Did the gentlelady from Texas want to ask a question since everybody else has asked theirs?

Ms. JACKSON LEE. Yes, Mr. Chairman. Thank you so very much.

First of all, I will ask unanimous consent to place in the record, not to the witnesses, but the headline reads, "Amazon Facial Recognition Mistakenly Confused 28 Congressmen with Known Criminals," July 26, 2018.

Chairman THOMPSON. Without objection.
[The information follows:]

ARTICLE SUBMITTED BY HONORABLE SHEILA JACKSON LEE

AMAZON FACIAL RECOGNITION MISTAKENLY CONFUSED 28 CONGRESSMEN WITH KNOWN CRIMINALS

By Sean Hollister, July 26, 2018, 12:45 PM PDT

https://www.cnet.com/news/amazon-facial-recognition-thinks-28-congressmen-look-like-known-criminals-at-default-settings/

The ACLU says it's evidence that Congress should step in. Amazon says the ACLU didn't test properly.

Amazon is trying to sell its Rekognition facial recognition technology to law enforcement, but the American Civil Liberties Union doesn't think that's a very good idea. And today, the ACLU provided some seemingly compelling evidence—by using Amazon's own tool to compare 25,000 criminal mugshots to Members of Congress.

Sure enough, Amazon's tool thought 28 different Members of Congress looked like people who've been arrested.

Here's the full list, according to the ACLU:

Senate:

Johnny Isakson (R–Georgia)
Ed Markey (D–Massachusetts)
Pat Roberts (R–Kansas)

House:

Sanford Bishop (D–Georgia)
G.K. Butterfield (D–North Carolina)
Lacy Clay (D–Missouri)
Mark DeSaulnier (D–California)
Adriano Espaillat (D–New York)
Ruben Gallego (D–Arizona)
Tom Garrett (R–Virginia)
Greg Gianforte (R–Montana)
Jimmy Gomez (D–California)
Raúl Grijalva (D–Arizona)
Luis Gutiérrez (D–Illinois)
Steve Knight (R–California)
Leonard Lance (R–New Jersey)
John Lewis (D–Georgia)
Frank LoBiondo (R–New Jersey)
Dave Loebsack (D–Iowa)
David McKinley (R–West Virginia)
John Moolenaar (R–Michigan)
Tom Reed (R–New York)
Bobby Rush (D–Illinois)
Norma Torres (D–California)
Marc Veasey (D–Texas)
Brad Wenstrup (R–Ohio)
Steve Womack (R–Arkansas)
Lee Zeldin (R–New York)

That's a lot of Congresspeople who may soon have some very valid questions about facial recognition and its potential to be abused—particularly since Amazon thinks the ACLU didn't use it properly to begin with! It turns out that the ACLU got its mugshot matches by using the Rekognition software at its default 80-percent confidence threshold setting, rather than the 95-percent-plus confidence level that Amazon recommends for law enforcement agencies.

It turns out that the ACLU got its mugshot matches by using the Rekognition software at its default 80-percent confidence threshold setting, rather than the 95-percent plus confidence level that Amazon recommends for law enforcement agencies.

"While 80 percent confidence is an acceptable threshold for photos of hot dogs, chairs, animals, or other social media use cases, it wouldn't be appropriate for identifying individuals with a reasonable level of certainty. When using facial recognition for law enforcement activities, we guide customers to set a threshold of at least 95 percent or higher," an Amazon spokesperson told CNET by email.

But an ACLU lawyer tells CNET that Amazon doesn't necessarily steer law enforcement agencies toward that higher threshold—if a police department uses the software, it'll be set to the same 80-percent threshold by default and won't ask them to change it even if they intend to use it to identify criminals. "Amazon makes no effort to ask users what they are using Rekognition for," says ACLU attorney Jacob Snow.

A source close to the matter tells CNET that when Amazon works with law enforcement agencies directly, like the Orlando Police Department, it teaches them how to reduce false positives and avoid human bias. But there's nothing to necessarily keep other agencies from simply using the tool the same way the ACLU did, instead of developing a relationship with Amazon.

It's worth noting that false positives are (currently!) an accepted part of facial recognition technology. Nobody—including the ACLU—is saying police would arrest someone based on a false match alone. Facial recognition narrows down the list of suspects, and then humans take over. Recently, facial recognition helped ID the Russian assassins who poisoned a spy in the UK, as well as the Capital Gazette shooter.

And Amazon didn't actually create that many false positives even at the 80 percent confidence ratio, compared to, say, the UK Metropolitan Police's facial recognition tech.

But the ACLU worries that Amazon's false positives might bias a police officer or government agent to search, question, or potentially draw a weapon when they shouldn't—and we've all seen how those encounters can turn deadly. And the ACLU notes that Amazon's tech seems to have over-represented people of color.

Should Congress regulate facial recognition? Microsoft thinks so, and now 28 Members of Congress have some very personal food for thought—95-percent confidence threshold or no.

In the hours since the ACLU's test was brought to light, five Congressmen have sent letters to Amazon CEO Jeff Bezos asking for answers and an immediate meeting. You can read the letters here.

Ms. JACKSON LEE. So, Mr. Wagner, I just wanted to ask you. Are you using Amazon technology?

Mr. WAGNER. We are not using their matching algorithm.

Ms. JACKSON LEE. Thank you, Mr. Chairman.

My question is you gave Congressman Langevin sort-of a detailed response. So let me try to change it around to: Do you have a team that is directly responsible not just for the implementation, but for the internal analysis of the utilization of the app or the technology that you are using so that it is on-site, so you are able to get first-hand knowledge of the violations or let me use the word "abuses" by way of the technology?

Is that information coming back to your office? When I say that, to your sector.

Mr. WAGNER. Yes. Part of it is our office that does it, and then working in conjunction with our field locations.

Ms. JACKSON LEE. So do you have a team that is just responding to that, if you would?

Mr. WAGNER. We have teams that review the data, review the reports, review the functioning of the systems, review the compliance of the officers using the technology, yes.

Ms. JACKSON LEE. Mr. Chairman, I will just say this. I know we have a lot of work. You have a lot of work. You do a lot, but maybe there could be a Classified briefing.

I would like to do a deeper dive on how that is done and how that is kept and whether they store, how long they keep the data on Mr. Jones or Mr. Aman and Mr. various named persons, how long they keep the data.

Chairman THOMPSON. Well, we will work through it.

Mr. WAGNER. The data is all stored in compliance with the Systems of Record Notices of where that data is stored. So the photograph of the U.S. citizen that we take is only stored for 12 hours and then purged.

A picture of a foreign national is sent over to IDENT, the Department's database, where it is stored for 75 years.

The record of the border crossing, the biographical information is then stored in other systems attributable to the System of Record Notices attributable to those.

Ms. JACKSON LEE. Very interesting. Thank you.

Chairman THOMPSON. We will follow up on your request.

Ms. JACKSON LEE. Thank you, witnesses. Thank you.

Chairman THOMPSON. Let me insert in the record a letter from the Electronic Privacy Information Center and a press release from the U.S. Travel Association.

[The information follows:]

LETTER FROM THE ELECTRONIC PRIVACY INFORMATION CENTER

February 5, 2020.

The Honorable BENNIE G. THOMPSON, Chairman,
The Honorable MIKE ROGERS, Ranking Member,
Committee on Homeland Security, U.S. House of Representatives, H2–176 Ford House Office Building, Washington, DC 20515.

DEAR CHAIRMAN THOMPSON AND RANKING MEMBER ROGERS: We write to you in advance of the hearing on "About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II."[1] EPIC supports a moratorium on facial recognition technology for mass surveillance. This committee should halt DHS's use of face surveillance technology.

The Electronic Privacy Information Center ("EPIC") is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC is focused on protecting individual privacy rights, and we are particularly interested in the privacy problems associated with surveillance.[3] Last year, EPIC filed a lawsuit against the Customs and Border Protection ("CBP") agency for failure to establish necessary privacy safeguards for the collection of facial images at U.S. borders.[4]

A CALL TO BAN FACE SURVEILLANCE

EPIC and the Public Voice Coalition are leading a global campaign to establish a moratorium on "face surveillance," the use of facial recognition for mass surveillance.[5] In October 2019 more than 100 NGO's and hundreds of experts endorsed our petition.[6] The signatories stated:

- We urge countries to suspend the further deployment of facial recognition technology for mass surveillance;
- We urge countries to review all facial recognition systems to determine whether personal data was obtained lawfully and to destroy data that was obtained unlawfully;
- We urge countries to undertake research to assess bias, privacy and data protection, risk, and cyber vulnerability, as well as the ethical, legal, and social implications associated with the deployment of facial recognition technologies; and
- We urge countries to establish the legal rules, technical standards, and ethical guidelines necessary to safeguard fundamental rights and comply with legal obligations before further deployment of this technology occurs.

Courts and regulators are also listening. There is growing awareness of the need to bring this technology to a halt. The State of California prohibited the use facial

[1] *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II,* House Comm. on Homeland Security, 116th Cong. (Feb. 6, 2020), *https://homeland.house.gov/activities/hearings/about-face-examining-the-department-of-homeland-securitys-use-of-facial-recognition-and-other-biometric-technologies-part-ii.*

[2] See About EPIC, EPIC.org, *https://epic.org/epic/about.html.*

[3] EPIC, *EPIC Domestic Surveillance Project, https://epic.org/privacy/surveillance/.*

[4] *EPIC* v. *U.S. Customs and Border Protection,* No. 19–cv–689 (D.D.C. filed Mar. 12, 2019); See *https://epic.org/foia/dhs/cbp/alt-screening-procedures/.*

[5] EPIC, *Ban Face Surveillance, https://epic.org/banfacesurveillance/.*

[6] The Public Voice, *Declaration: A Moratorium on Facial Recognition Technology for Mass Surveillance Endorsements, https://thepublicvoice.org/ban-facial-recognition/endorsement/.*

recognition on police-worn body cameras. Several cities in the U.S. have banned the use of facial recognition systems, and there is a growing protest around the world. For example, In 2019 the Swedish Data Protection Authority prohibited the use of facial recognition in schools. EPIC has published a resource of laws, regulations, legal decisions and reports on face surveillance worldwide at *https://epic.org/banfacesurveillance/.*

THREATS TO PRIVACY AND CIVIL LIBERTIES

Facial recognition poses serious threats to privacy and civil liberties and can be deployed covertly, remotely, and on a mass scale. There is a lack of well-defined regulations controlling the collection, use, dissemination, and retention of biometric identifiers. Ubiquitous identification by commercial or Government entities eliminates the individual's ability to control the disclosure of their identities, creates new opportunities for tracking and monitoring, increases the security risks from data breaches. An individual's ability to control disclosure of his or her identity is an essential aspect of personal freedom and autonomy. The use of facial recognition erodes these freedoms.

There is little a person in the United States could do to prevent the capture of their image by the Government or a private company if face surveillance is deployed. Participation in society necessarily requires participation in public spaces. But ubiquitous and near effortless identification eliminates the individual's ability to control the disclosure of their identities to others. Strangers will know our identities as readily as our friends and family members.

USE OF FACE SURVEILLANCE IN CHINA

Face surveillance capabilities have been on full display in China. China is not only the leading government for face surveillance technology, it is also the leading exporter of the technology.[7] The Chinese government has implemented a massive facial recognition surveillance system.[8] China has leveraged its surveillance network to implement an "advanced facial recognition technology to track and control the Uighurs, a largely Muslim minority."[9] And China continues to expand the use of facial recognition technology. A university in China is testing the use of facial recognition to monitor whether students attend classes and to track their attention during lectures.[10] To register a new mobile phone number in China now requires one to submit to a facial scan.[11] Trials have also begun to use facial recognition at security checkpoints in the subway system.[12]

In Hong Kong, where protests have been on-going since March, face scans have become a weapon. Protesters fear that facial recognition technology is being used to identify and track them.[13] In response to this fear, protesters have resorted to covering their faces and have taken down facial recognition cameras. Hong Kong reacted by banning masks and face paint.[14] Many of the demonstrators worry that the mass surveillance implemented on the mainland of China will be implemented in Hong Kong.

[7] Steven Feldstein, *The Global Expansion of AI Surveillance* 13–15 (Sept. 2019), *https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.*

[8] Simon Denyer, *China's Watchful Eye,* Wash. Post (Jan. 7, 2018), *https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/.*

[9] Paul Mozur, *One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority,* N.Y. Times (Apr. 14, 2019), *https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.*

[10] Brendan Cole, *Chinese University Tests Facial Recognition System to Monitor Attendance and Students' Attention to Lectures,* Newsweek (Sept. 2, 2019), *https://www.newsweek.com/nanjing-china-facial-recognition-1457193.*

[11] Kyle Wiggers, *AI Weekly: In China, You Can No Longer Buy a Smartphone without a Face Scan,* VentureBeat (Oct. 11, 2019), *https://venturebeat.com/2019/10/11/ai-weekly-in-china-you-can-no-longer-buy-a-smartphone-without-a-face-scan/.*

[12] Wan Lin, *Beijing Subway Station Trials Facial Recognition,* Global Times (Dec. 1, 2019), *http://www.globaltimes.cn/content/1171888.shtml.*

[13] Paul Mozur, *In Hong Kong Protests, Faces Become Weapons,* N.Y. Times (July 26, 2019), *https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html.*

[14] Matt Novak, *Hong Kong Announces Ban on Masks and Face Paint That Helps Protesters Evade Facial Recognition,* Gizmodo (Oct. 4, 2019), *https://gizmodo.com/hong-kong-announces-ban-on-masks-and-face-paint-that-he-1838765030.*

FACE SURVEILLANCE IN THE UNITED STATES

The implementation of facial recognition technology by Government and commercial actors in the United States is pushing the U.S. toward a similar mass surveillance infrastructure. Already some schools are implementing the use of facial recognition technology.[15] Customs and Border Protection (CBP) is using facial recognition on travelers entering and exiting the U.S.[16] And airlines are using CBP's facial recognition system to conduct flight check-ins, check bags, and board flights.[17] The Rochester airport has implemented the surveillance infrastructure to perform facial recognition on every person that enters the airport.[18] Amazon drafted plans to use their Ring surveillance cameras to create neighborhood watch lists that leverage facial recognition.[19] Retailers have implemented the use of facial recognition at their stores.[20] A landlord in Brooklyn wanted to use facial recognition as the means to gain entry into a rent-stabilized apartment building.[21] Facial recognition is being used at major sporting events[22] and concerts.[23] And the companies that are creating the facial recognition algorithms are often using—without consent—millions of photos scraped from social media sites and other webpages in order train the algorithms.[24]

It is important to note that not all uses of facial recognition are equally problematic. For instance, where the user has control and there is no Government mandate, such as using Face ID for iPhone authentication, the same privacy issues do not arise. Facial recognition can also be used for verification or authentication using 1:1 matching—that is, where the system does not check every record in a database for a match, but matches the individual's face to their claimed identity.[25] This 1:1 matching is a much more privacy protective implementation of facial recognition. 1:1 matching does not require a massive biometric database, there is no need to retain the image, and the machines conducting the 1:1 match do not need to be connected to the cloud. Such an implementation virtually eliminates data breach risks and the chance of mission creep.

FACE SURVEILLANCE IN AIRPORTS

Recently, new privacy risks have arisen with the deployment of facial recognition technology at U.S. airports following a 2017 Executive Order to "expedite the completion and implementation of biometric entry exit tracking system."[26] Customs and Border Protection ("CBP") has now implemented the Biometric Entry-Exit program

[15] Tom Simonite and Gregory Barber, *The Delicate Ethics of Using Facial Recognition in Schools,* Wired (Oct. 17, 2019), *https://www.wired.com/story/delicate-ethics-facial-recognition-schools/.*

[16] Davey Alba, *The US Government Will Be Scanning Your Face At 20 Top Airports, Documents Show,* BuzzFeed (Mar. 11, 2019), *https://www.buzzfeednews.com/article/daveyalba/these-documents-reveal-the-governments-detailed-plan-for?ref=bfnsplash.*

[17] See, e.g., Kathryn Steele, *Delta Unveils First Biometric Terminal in U.S. in Atlanta; next stop: Detroit,* Delta News Hub, *https://news.delta.com/delta-unveils-first-biometric-terminal-us-atlanta-next-stop-detroit.*

[18] James Gilbert, *Facial Recognition Heading to Rochester Airport Despite Concerns,* Rochester First (June 26, 2019), *https://www.rochesterfirst.com/news/local-news/facial-recognition-heading-to-airport-despite-concerns/.*

[19] Sam Biddle, *Amazon's Ring Planned Neighborhood "Watch Lists " Built on Facial Recognition,* The Intercept (Nov. 26, 2019), *https://theintercept.com/2019/11/26/amazon-ring-home-security-facial-recognition/.*

[20] Nick Tabor, *Smile! The Secretive Business of Facial-Recognition Software in Retails Stores,* New York Intelligencer (Oct. 20, 2018), *http://nymag.com/intelligencer/2018/10/retailers-are-using-facial-recognition-technology-too.html.*

[21] Gina Bellafante, *The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?,* N.Y. Times (Mar. 28, 2019), *https://www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html.*

[22] Ryan Rodenberg, *Sports Betting and Big Brother: Rise of Facial Recognition Cameras,* ESPN (Oct. 3, 2018), *https://www.espn.com/chalk/story/__/id/24884024/why-use-facial-recognition-cameras-sporting-events-the-rise.*

[23] Steve Knopper, *Why Taylor Swift Is Using Facial Recognition at Concerts,* Rolling Stone (Dec. 13, 2018), *https://www.rollingstone.corn/music/music-news/taylor-swift-facial-recognition-concerts-768741/.*

[24] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It,* N.Y. Times (Jan. 18, 2020), *https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.*

[25] Lucas D. lntrona and Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues,* Ctr. for Catastrophe Preparedness & Response, N.Y. Univ., 11 (2009), available at *https://nissenbaum.tech.cornell.edu/papers/facial__recognition__report.pdf.*

[26] Exec. Order No. 13,780 § 8.

for international travelers at 17 airports.[27] TSA is quickly moving to leverage CBP's Biometric Entry-Exit program to expand the use of facial recognition at airports.[28]

TSA has already deployed facial recognition technology at two TSA Checkpoints.[29] In September 2018, TSA released a "TSA Biometrics Roadmap," detailing its plans to use facial recognition, including on domestic travelers.[30] The Roadmap makes clears TSA's intention to leverage CBP's facial recognition capabilities implemented as part of the Biometric Entry-Exit Program. But corresponding privacy safeguards have not yet been established.

In response to EPIC's Freedom of Information Act request, CBP recently released 346 pages of documents detailing the agency's scramble to implement the flawed Biometric Entry-Exit system, a system that employs facial recognition technology on travelers entering and exiting the country. The documents obtained by EPIC describe the administration's plan to extend the faulty pilot program to major U.S. airports. The documents obtained by EPIC were covered in-depth by Buzzfeed.[31]

Based on the documents obtained, EPIC determined that there are few limits on how airlines will use the facial recognition data collected at airports.[32] Only recently has CBP changed course and indicated that the agency will require airlines to delete the photos they take for the Biometric Entry-Exit program.[33] No such commitment has been made by TSA. Indeed, TSA's Roadmap indicates that the agency wants to expand the dissemination of biometric data as much as possible, stating:

> "TSA will pursue a system architecture that promotes data sharing to maximize biometric adoption throughout the passenger base and across the aviation security touch points of the passenger experience."[34]

TSA seeks to broadly implement facial recognition through "public-private partnerships" in an effort to create a "biometrically-enabled curb-to-gate passenger experience."[35] Currently, TSA plans to implement an opt-in model of facial recognition use for domestic travelers but there are no guarantees that in the future TSA will not require passengers to participate in facial recognition or make the alternative so cumbersome as to essentially require passengers to opt-in.

Preserving the ability of U.S. citizens to forgo facial recognition for alternative processes is one of the privacy issues with CBP's Biometric Entry-Exit program. Senator Markey (D–MA) and Senator Lee (R–UT) called for the CBP to suspend facial recognition at the border to ensure that travelers are able to opt out of facial recognition if they wish.[36]

In fact, EPIC recently sued CBP for all records related to the creation and modification of alternative screening procedures for the Biometric Entry-Exit program.[37] The alternative screening procedure for U.S. travelers that opt out of facial recognition should be a manual check of the traveler's identification documents. CBP, however, has provided vague and inconsistent descriptions of alternative screening pro-

[27] Davey Alba, *The US Government Will Be Scanning Your Face At 20 Top Airports, Documents Show* (Mar. 11, 2019), *https://www.buzzfeednews.corn/article/daveyalba/these-documents-reveal-the-governments-detailed-plan-for.*

[28] TSA, *TSA Biometrics Roadmap* (Sept. 2018), *https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.*

[29] Trans. Security Admin., Travel Document Checker Automation Using Facial Recognition, (Aug. 2019), *https://www.dhs.gov/publication/dhstsapia-046-travel-document-checker-automation-using-facial-recognition;* U.S. Customs and Border Protection, *CBP Deploys Facial Recognition Biometric Technology at 1 TSA Checkpoint at JFK Airport* (Oct. 11, 2017), *https://www.cbp.gov/newsroom/national-media-release/cbp-deploys-facial-recognition-biometric-technology-1-tsa-checkpoint.*

[30] TSA, *TSA Biometrics Roadmap* (Sept. 2018), *https ://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.*

[31] Davey Alba, *The US Government Will Be Scanning Your Face At 20 Top Airports, Documents Show* (Mar. 11, 2019), *https://www.buzzfeednews.com/article/daveyalba/these-documents-reveal-the-govemments-detailed-plan-for.*

[32] See CBP Memorandum of Understanding Regarding Biometric Pilot Project, *https://epic.org/foia/dhs/cbp/biometric-entry-exit/MOU-Biometric-Pilot-Project.pdf.*

[33] Ashley Ortiz, CBP Program and Management Analyst, Presentation before the Data Privacy & Integrity Advisory Committee, slide 23 (Dec. 2018), *https://www.dhs.gov/sites/default/files/publications/SLIDES-DPIAC-Public%20Meeting%2012%2010-2018.pdf.*

[34] TSA, *TSA Biometrics Roadmap,* 17 (Sept. 2018).

[35] Id. at 19.

[36] Press Release, Sens. Edward Markey and Mike Lee, *Senators Markey and Lee Call for Transparency on DHS Use of Facial Recognition Technology* (Mar. 12, 2019), *https://www.markey.senate.gov/news/press-releases/senators-markey-and-lee-call-for-transparency-on-dhs-use-of-facial-recognition-technology.*

[37] *EPIC* v. *CBP,* 19–cv–00689, *Complaint, https://epic.org/foia/cbp/altemative-screening-procedures/1-Complaint.pdf.*

cedures in both its "Biometric Exit Frequently Asked Questions (FAQ)" webpage[38] and the agency's privacy impact assessments.[39] The creation and modification of CBP's alternative screening procedures underscores CBP's unchecked ability to modify alternative screening procedures while travelers remain in the dark about how to protect their biometric data.

FACE SURVEILLANCE AND AI

It is also becoming increasingly clear that AI tools are being deployed with facial recognition to accelerate the deployment of technology not only for identification but also for scoring. As we explained recently in the *New York Times,* "The United States must work with other democratic countries to establish red lines for certain AI applications and ensure fairness, accountability, and transparency as AI systems are deployed."[40] In a subsequent letter to the *New York Times,* we warned of the growing risk of the Chinese AI model, and specifically explained, "China also dominates the standards-setting process for techniques like facial recognition."[41]

Society is simply not in a place right now for the wide-scale deployment of facial recognition technology. It would be a mistake to deploy facial recognition at this time. We urge the committee to support a ban of DHS's further deployment of face surveillance technology.

We ask that this statement be entered in the hearing record. EPIC looks forward to working with the committee on these issues of vital importance to the American public.

Sincerely,

MARC ROTENBERG,
EPIC President.

CAITRIONA FITZGERALD,
EPIC Policy Director.

JERAMIE SCOTT,
EPIC Senior Counsel.

Attachment.—*Declaration: A Moratorium on Facial Recognition Technology for Mass Surveillance*, The Public Voice, Tirana Albania (October 2019).

ATTACHMENT.—DECLARATION: A MORATORIUM ON FACIAL RECOGNITION TECHNOLOGY FOR MASS SURVEILLANCE

October 2019, Tirana, Albania

We the undersigned call for a moratorium on the use of facial recognition technology that enables mass surveillance.

We recognize the increasing use of this technology for commercial services, Government administration, and policing functions. But the technology has evolved from a collection of niche systems to a powerful integrated network capable of mass surveillance and political control.

Facial recognition is now deployed for human identification, behavioral assessment, and predictive analysis.

Unlike other forms of biometric technology, facial recognition is capable of scrutinizing entire urban areas, capturing the identities of tens or hundreds of thousands of people at any one time.

[38] CBP, *Biometric Exit Frequently Asked Questions (FAQs), https://www.cbp.gov/travel/biometrics/biometric-exit-faqs.*

[39] U.S. Dep't of Homeland Sec., DHS/CBP/PIA–030(b), *Privacy Impact Assessment Update for the Traveler Verification Service (TVS): Partner Process* 8 (2017), *https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-may2017.pdf;* see also U.S. Dep't of Homeland Sec., DHS/CBP/PIA–030(c), Privacy Impact Assessment Update for the Traveler Verification Service (TVS): Partner Process 5–6 (2017), *https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-appendixb-july2018.pdf;* U.S. Dep't of Homeland Sec., DHS/CBP/PIA–056, *Privacy Impact Assessment for the Traveler Verification Service* 2 (2018), *https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-0-tvs-november2018__2.pdf.*

[40] Marc Rotenberg, *The Battle Over Artificial Intelligence,* N.Y. Times, Apr. 18, 2019, *https://www.nytimes.com/2019/04/18/opinion/letters/artificial-intelligence.html.* In the introduction to the EPIC AI Policy Sourceboook and in a subsequent letter to the *New York Times,* we warned of the growing risk of the Chinese AI model. Marc Rotenberg and Len Kennedy, *Surveillance in China: Implications for Americans,* N.Y. Times, Dec. 19, 2019, *https://www.nytimes.com/2019/12/19/opinion/letters/surveillance-china.html.*

[41] Marc Rotenberg and Len Kennedy, *Surveillance in China: Implications for Americans,* N.Y. Times, Dec. 19, 2019, *https://www.nytimes.com/2019/12/19/opinion/letters/surveillance-china.html.*

Facial recognition can amplify identification asymmetry as it tends to be invisible or at best, opaque.

Facial recognition can be deployed in almost every dimension of life, from banking and commerce to transportation and communications.

We acknowledge that some facial recognition techniques enable authentication for the benefit of the user. However facial recognition also enables the development of semi-autonomous processes that minimize the roles of humans in decision making.

We note with alarm recent reports about bias, coercion, and fraud in the collection of facial images and the use of facial recognition techniques. Images are collected and used with forced consent or without consent at all.

We recall that in the 2009 Madrid Declaration, civil society called for a moratorium on the development or implementation of facial recognition, subject to a full and transparent evaluation by independent authorities and through democratic debate.

There is growing awareness of the need for a moratorium. In 2019 the Swedish Data Protection Authority prohibited the use of facial recognition in schools. The State of California prohibited the use facial recognition on police-worn body cameras. Several cities in the United States have banned the use of facial recognition systems, and there is growing protest around the world.

Therefore:

1. We urge countries to suspend the further deployment of facial recognition technology for mass surveillance;
2. We urge countries to review all facial recognition systems to determine whether personal data was obtained lawfully and to destroy data that was obtained unlawfully;
3. We urge countries to undertake research to assess bias, privacy and data protection, risk, and cyber vulnerability, as well as the ethical, legal, and social implications associated with the deployment of facial recognition technologies; and
4. We urge countries to establish the legal rules, technical standards, and ethical guidelines necessary to safeguard fundamental rights and comply with legal obligations before further deployment of this technology occurs.

https://thepublicvoice.org/ban-facial-recognition/

News Release, U.S. Travel Association

U.S. Travel Reacts to Suspension of Global Entry for New York Residents

WASHINGTON (February 6, 2020).—U.S. Travel Association Executive Vice President for Public Affairs and Policy Tori Emerson Barnes issued the following statement on the reported suspension of Global Entry and several other trusted traveler programs for residents of the State of New York:

"Travel should not be politicized. Trusted traveler programs enhance our national security because they provide greater certainty regarding a person's identity, citizenship, and criminal background. Suspending enrollment in Global Entry and other trusted traveler programs only undermines travel security and efficiency. We are in contact with the Department of Homeland Security to convey this message."

Contacts

Chris Kennedy: (O) 202.218.3603 (C) 202.465.6635
Tim Alford: (O) 202.218.3625 (C) 740.215.1290

###

U.S. Travel Association is the national, non-profit organization representing all components of the travel industry that generates $2.5 trillion in economic output and supports 15.7 million jobs. U.S. Travel's mission is to increase travel to and within the United States. Visit www.ustravel.org.

Chairman Thompson. Mr. Wagner, if you are aware of any notification requirements that a State would be noticed, I am talking about the global entry situation because it looks like New York is just the first of 1 or 2 others.

Since we have been sitting here, Mr. Cuccinelli has said Washington State might be in a similar position.

I am just wanting to make sure that if this is the way forward, then surely, in light of what Mr. Rose and some of the other New

Yorkers on this committee have said, there should be some notice that this is about to happen and not just a press conference.

So if you are aware of any, please get it back to us in the committee. We would love to have it.

I thank the witnesses for their valuable testimony and the Members for their questions.

The Members of the committee may have additional questions for the witnesses, and we ask that you respond expeditiously, in writing, to those questions.

Without objection, the committee record will be kept open for 10 days.

Hearing no further business, the committee stands adjourned.

[Whereupon, at 12:15 p.m., the committee was adjourned.]

○