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

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

JULY 10, 2019

Serial No. 116–31

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

38–784 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
JOHN RATCLIFFE, Texas
MARK WALKER, North Carolina
CLAY HIGGINS, Louisiana
DEBBIE LESKO, Arizona
MARK GREEN, Tennessee
VAN TAYLOR, Texas
JOHN JOYCE, Pennsylvania
DAN CRENSHAW, Texas
MICHAEL GUEST, Mississippi

HOPE GOINS, *Staff Director*
CHRIS VIESON, *Minority Staff Director*

CONTENTS

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

Wednesday, July 10, 2019

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

The committee met, pursuant to notice, at 10:01 a.m., in room 310, Cannon House Office Building, Hon. Bennie G. Thompson (Chairman of the committee) presiding.

Present: Representatives Thompson, Jackson Lee, Langevin, Richmond, Payne, Correa, Torres Small, Rose, Underwood, Slotkin, Cleaver, Green of Texas, Clarke, Watson Coleman, Barragán, Demings, Rogers, McCaul, Katko, Walker, Higgins, Lesko, Green of Tennessee, Taylor, Joyce, and Guest.

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

I now recognize myself for an opening statement.

Good morning. The Committee on Homeland Security is meeting to examine the Department of Homeland Security's use of facial recognition and other biometric technologies. The Government's use of biometrics is not entirely new. For example, fingerprints have been used as an identification tool for many decades. Other biometrics include DNA, voice pattern, and palm prints. In recent years, facial recognition has become the new chosen form of biometric technology.

As facial recognition technology has advanced, its use by the Government and the private sector has also increased. Currently, DHS is collecting and storing several different kinds of biometric information and is using this information for multiple purposes. CBP and TSA are using biometrics to conform the identities of travelers, for example. The Secret Service is piloting a surveillance system using facial recognition.

I am not opposed to biometric technology and recognize it can be valuable to Homeland Security in facilitation. However, its proliferation across DHS raises serious questions about privacy, data security, transparency, and accuracy. The American people deserve

answers to those questions before the Federal Government rushes to deploy biometrics further.

Last month, the committee held roundtable discussions with both industry and privacy and civil liberty stakeholders about the Department of Homeland Security's increasing use of biometric technology. Stakeholders have sufficient concerns that the data DHS is collecting and whether the Department is safeguarding our rights appropriately. They have good reasons to be concerned.

Absent standards, Americans may not know when, where, or why the Department is collecting their biometrics. People also may not know that they have the right to opt out or how to do so. Worse yet, they may not know that biometric technology is in use as it is the case when face recognition is used to passively surveil a crowd like under the Secret Service's pilot program.

Recent reports also indicate ICE has been scanning through millions of Americans' driver's license photos without their knowledge or consent. These troubling reports are a stark reminder that biometric technologies should only be used for authorized purposes in a fully transparent manner.

Data security is another important concern. Frankly, the Federal Government does not have a great track record securing Americans' personal data, and biometric information can be particularly insensitive. Unfortunately, earlier this year, a CBP subcontractor experienced a significant data breach, including travelers' images, raising important questions about data security.

Americans want to know that, if the Government collects their biometric data, they are going to keep it secure from hackers and other bad actors. Moreover, the accuracy of certain biometric technology is in question. Despite advancement in recent years, studies by highly-regarded academic institutions have found facial recognition systems in particular are not as accurate for women and darker-skinned individuals.

Last July, the American Civil Liberties Union conducted a test using Amazon's facial recognition tool, called Rekognition. ACLU built a database of 25,000 publicly-available arrest photos. Using Rekognition, the ACLU searched the database using pictures of every current Member of Congress. That software incorrectly matched 28 Members with individuals who had criminal records. Although the misidentified Members included both Democrats and Republicans, men and women, and a wide range of ages, nearly 40 percent of the false matches were people of color. This is unacceptable. It is not fair to expect certain people in our society to shoulder a disproportionate burden of the technology's shortcoming. Before the Government deploys these technologies further, they must be scrutinized, and the American public needs to be given a chance to weigh in.

Biometrics and facial recognition technology may be a useful Homeland Security and facilitation tool, but as with any tool, it has the potential to be misused, especially if it falls into the wrong hands.

Today the committee will hear from Federal witnesses on this important topic. I am pleased that we have witnesses from Customs and Border Protection, the Transportation Security Administration, the Secret Service, and the National Institute of Standards

and Technology before us. They represent just a few of the agencies involved in the Government's increasing use of biometric technology.

I look forward to hearing from them about how they are using biometric technology currently, their future plans, and what they are doing to address these concerns. As Congress, it is our job to ensure they protect the rights of the American people before they move forward. I expect a good conversation toward that end today and continued oversight by the committee in the future.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

JULY 10, 2019

The Government's use of biometrics is not entirely new. For example, fingerprints have been used as an identification tool for many decades. Other biometrics include DNA, irises, voice patterns, and palm prints. In recent years, facial recognition has become the new, chosen form of biometric technology. As facial recognition technology has advanced, its use by the Government and the private sector has also increased. Currently, DHS is collecting and storing several different kinds of biometric information and is using this information for multiple purposes. CBP and TSA are using biometrics to confirm the identities of travelers, for example. The Secret Service is piloting a surveillance system using facial recognition. I am not opposed to biometric technology, and recognize it can be valuable to homeland security and facilitation. However, its proliferation across DHS raises serious questions about privacy, data security, transparency, and accuracy. The American people deserve answers to those questions before the Federal Government rushes to deploy biometrics further.

Last month, the committee held roundtable discussions with both industry and privacy and civil liberty stakeholders about the Department of Homeland Security's increasing use of biometric technology. Stakeholders have significant concerns about the data DHS is collecting and whether the Department is safeguarding our rights appropriately. They have good reason to be concerned. Absent standards, Americans may not know when, where, or why the Department is collecting their biometrics. People also may not know that they have the right to opt out, or how to do so. Worse yet, they may not know that biometric technology is in use, as is the case when face recognition is used to passively surveil a crowd like under the Secret Service's pilot program. Recent reports also indicate ICE has been scanning through millions of Americans' drivers' license photos without their knowledge or consent. These troubling reports are a stark reminder that biometric technologies should only be used for authorized purposes in a fully transparent manner.

Data security is another important concern. Frankly, the Federal Government does not have a great track record securing Americans' personal data, and biometric information can be particularly sensitive. Unfortunately, earlier this year, a CBP subcontractor experienced a significant data breach, including traveler images, raising important questions about data security. Americans want to know that if the Government collects their biometric data, they are going to keep it secure from hackers and other bad actors. Moreover, the accuracy of certain biometric technology is in question, despite advancement in recent years. Studies by highly regarded academic institutions have found facial recognition systems in particular are not as accurate for women and darker-skinned individuals. Last July, the American Civil Liberties Union (ACLU) conducted a test using Amazon's facial recognition tool called "Rekognition." The ACLU built a database of 25,000 publicly available arrest photos. Using Rekognition, the ACLU searched the database using pictures of every current Member of Congress. The software incorrectly matched 28 Members with individuals who had criminal records. Although the misidentified members included both Democrats and Republicans, men and women, and a wide range of ages, nearly 40 percent of the false matches were people of color. This is unacceptable.

It is not fair to expect certain people in our society to shoulder a disproportionate burden of the technology's shortcomings. Before the Government deploys these technologies further, they must be scrutinized and the American public needs to be given a chance to weigh in. Biometrics and facial recognition technology may be a useful homeland security and facilitation tool, but as with any tool it has the potential to be misused—especially if it falls into the wrong hands. Today, the Committee will hear from Federal witnesses on this important topic. I am pleased that we have

witnesses from Customs and Border Protection (CBP), the Transportation Security Administration (TSA), the Secret Service, and the National Institute of Standards and Technology (NIST) before us. They represent just a few of the agencies involved in the Government's increasing use of biometric technology. I look forward to hearing from them about how they are using biometric technology currently, their plans for the future, and what they are doing to address these concerns. As Congress, it is our job to ensure they protect the rights of the American people before they move forward.

Chairman THOMPSON. I ask unanimous consent to enter the following news articles and letters into the hearing's record: A June 10 *Washington Post* article entitled "U.S. Customs and Border Protection Say Its Photos of Travelers Were Taken in a Data Breach"; a July 7 *Washington Post* article entitled "FBI ICE Find State Driver's Licenses Photos Are a Gold Mine of Facial Recognition Searches"; and July 9 letters from American Association of Airport Executives, International Biometric Identity Association, and a coalition of privacy and civil liberties groups, many of whom were represented in our meetings and briefings last month.

Without objection, so ordered.

[The information follows:]

U.S. CUSTOMS AND BORDER PROTECTION SAYS PHOTOS OF TRAVELERS WERE TAKEN IN A DATA BREACH

By Drew Harwell and Geoffrey A. Fowler, June 10, 2019 at 7:54 p.m. EDT, Washington Post.

U.S. Customs and Border Protection officials said Monday that photos of travelers had been compromised as part of a "malicious cyberattack," raising concerns over how Federal officials' expanding surveillance efforts could imperil Americans' privacy.

Customs officials said in a statement Monday that the images, which included photos of people's faces and license plates, had been compromised as part of an attack on a Federal subcontractor.

CBP makes extensive use of cameras and video recordings at airports and land border crossings, where images of vehicles are captured. Those images are used as part of a growing agency facial-recognition program designed to track the identity of people entering and exiting the U.S.

Fewer than 100,000 people were impacted, said CBP, citing "initial reports." The photographs were taken of people in vehicles entering and exiting the U.S. over a month and a half through a single land border entry port, which CBP did not name. Officials said the stolen information did not include other identifying information, and no passport or other travel document photos were compromised.

The agency learned of the breach on May 31 and said that none of the image data had been identified "on the Dark Web or Internet." But reporters at *The Register,* a British technology news site, reported late last month that a large haul of breached data from the firm Perceptics was being offered as a free download on the dark web.

CBP would not say which subcontractor was involved. But a Microsoft Word document of CBP's public statement, sent Monday to *Washington Post* reporters, included the name "Perceptics" in the title: "CBP Perceptics Public Statement."

Perceptics representatives did not immediately respond to requests for comment.

CBP spokeswoman Jackie Wren said she was "unable to confirm" if Perceptics was the source of the breach.

One U.S. official, who spoke on condition of anonymity due to lack of authorization to discuss the breach, said it was being described inside CBP as a "major incident." The official said Perceptics was attempting to use the data to refine its algorithms to match license plates with the faces of a car's occupants, which the official said was outside of CBP's sanctioned use. The official said the data involved travelers crossing the Canadian border.

The breach, according to the official, did not involve a foreign nation, such as when China hacked the Office of Personnel Management in 2014 exposing the sensitive information of at least 22 million people.

News of the breach raised alarms in Congress, where lawmakers have questioned whether the government's expanded surveillance measures could threaten constitutional rights and open millions of innocent people to identity theft.

"If the government collects sensitive information about Americans, it is responsible for protecting it—and that's just as true if it contracts with a private company," Sen. Ron Wyden (D–Ore.) said in a statement to *The Post.* "Anyone whose information was compromised should be notified by Customs, and the government needs to explain exactly how it intends to prevent this kind of breach from happening in the future."

Wyden said the theft of the data should alarm anyone who has advocated expanded surveillance powers for the government. "These vast troves of Americans' personal information are a ripe target for attackers," he said.

Civil rights and privacy advocates also called the theft of the information a sign that the government's growing database of identifying imagery had become an alluring target for hackers and cybercriminals.

"This breach comes just as CBP seeks to expand its massive face recognition apparatus and collection of sensitive information from travelers, including license plate information and social media identifiers," said Neema Singh Guliani, senior legislative counsel at the American Civil Liberties Union. "This incident further underscores the need to put the brakes on these efforts and for Congress to investigate the agency's data practices. The best way to avoid breaches of sensitive personal data is not to collect and retain it in the first place."

CBP said copies of "license plate images and traveler images collected by CBP" had been transferred to the subcontractor's company network, violating the agency's security and privacy rules. The subcontractor's network was then attacked and breached. No CBP systems were compromised, the agency said.

Perceptics and other companies offer automated license-plate-reading devices that Federal officials can use to track a vehicle, or its owner, as it travels on public roads.

Immigration agents have used such databases to track down people who may be in the country illegally. Police agencies have also used the data to look for potential criminal suspects.

Perceptics, based in Tennessee, has championed its technology as a key part of keeping the border secure. "You want technology that generates data you can trust and delivers it when and where you need it most," a marketing website says.

The company also said recently that it had installed license-plate readers at 43 U.S. Border Patrol checkpoint lanes across Arizona, California, New Mexico and Texas, saying they offered border guards "superior images with the highest license plate read rate accuracy in North America."

The Federal Government, as well as the group of private contractors it works with, has access to a swelling database of people's cars and faces, which it says is necessary to enhance security and enforce border laws.

The FBI has access to more than 640 million photos, including from passports and driver's licenses, that it can scan with facial-recognition systems while conducting criminal investigations, a representative for the Government Accountability Office told the House Committee on Oversight and Reform at a hearing last week.

Rep. Bennie Thompson (D–Miss.), chair of the House Homeland Security Committee, said he intended to hold hearings next month on Homeland Security's use of biometric information.

"Government use of biometric and personal identifiable information can be valuable tools only if utilized properly. Unfortunately, this is the second major privacy breach at DHS this year," Thompson said, referring to a separate breach in which more than 2 million U.S. disaster survivors had their information revealed by the Federal Emergency Management Agency. "We must ensure we are not expanding the use of biometrics at the expense of the privacy of the American public. "

Nick Miroff, Ellen Nakashima and Tony Romm contributed to this report.

FBI, ICE FIND STATE DRIVER'S LICENSE PHOTOS ARE A GOLD MINE FOR FACIAL-RECOGNITION SEARCHES

By Drew Harwell, July 7, 2019 at 3:54 p.m. EDT, The Washington Post

Agents with the Federal Bureau of Investigation and Immigration and Customs Enforcement have turned State driver's license databases into a facial-recognition gold mine, scanning through millions of Americans' photos without their knowledge or consent, newly released documents show.

Thousands of facial-recognition requests, internal documents and emails over the past 5 years, obtained through public-records requests by researchers with George-

town Law's Center on Privacy and Technology and provided to *The Washington Post,* reveal that Federal investigators have turned state departments of motor vehicles data bases into the bedrock of an unprecedented surveillance infrastructure.

Police have long had access to fingerprints, DNA and other "biometric data" taken from criminal suspects. But the DMV records contain the photos of a vast majority of a state's residents, most of whom have never been charged with a crime.

Neither Congress nor state legislatures have authorized the development of such a system, and growing numbers of Democratic and Republican lawmakers are criticizing the technology as a dangerous, pervasive and error-prone surveillance tool.

"Law enforcement's access of state databases," particularly DMV databases, is "often done in the shadows with no consent," House Oversight Committee Chairman Elijah E. Cummings (D–Md.) said in a statement to The Post.

Rep. Jim Jordan (Ohio), the House Oversight Committee's ranking Republican, seemed particularly incensed during a hearing into the technology last month at the use of driver's license photos in Federal facial-recognition searches without the approval of state legislators or individual license holders.

"They've just given access to that to the FBI," he said. "No individual signed off on that when they renewed their driver's license, got their driver's licenses. They didn't sign any waiver saying, 'Oh, it's OK to turn my information, my photo, over to the FBI.' No elected officials voted for that to happen."

Despite those doubts, Federal investigators have turned facial recognition into a routine investigative tool. Since 2011, the FBI has logged more than 390,000 facial-recognition searches of Federal and local databases, including state DMV databases, the Government Accountability Office said last month, and the records show that Federal investigators have forged daily working relationships with DMV officials. In Utah, FBI and ICE agents logged more than 1,000 facial-recognition searches between 2015 and 2017, the records show. Names and other details are hidden, though dozens of the searches are marked as having returned a "possible match."

San Francisco and Somerville, Mass., have banned their police and public agencies from using facial-recognition software, citing concerns about governmental overreach and a breach of public trust, and the subject is being hotly debated in Washington. On Wednesday, officials with the Transportation Security Administration, Customs and Border Protection and the Secret Service are expected to testify at a hearing of the House Committee on Homeland Security about their agencies' use of the technology.

The records show the technology already is tightly woven into the fabric of modern law enforcement. They detailed the regular use of facial recognition to track down suspects in low-level crimes, including cashing a stolen check and petty theft. And searches are often executed with nothing more formal than an email from a Federal agent to a local contact, the records show.

"It's really a surveillance-first, ask-permission-later system," said Jake Laperruque, a senior counsel at the watchdog group Project on Government Oversight. "People think this is something coming way off in the future, but these [facial-recognition] searches are happening very frequently today. The FBI alone does 4,000 searches every month, and a lot of them go through state DMVs."

The records also underscore the conflicts between the laws of some states and the Federal push to find and deport undocumented immigrants. Though Utah, Vermont and Washington allow undocumented immigrants to obtain full driver's licenses or more-limited permits known as driving privilege cards, ICE agents have run facial-recognition searches on those DMV databases.

More than a dozen states, including New York, as well as the District of Columbia, allow undocumented immigrants to drive legally with full licenses or driving privilege cards, as long as they submit proof of in-state residency and pass the states' driving-proficiency tests.

Lawmakers in Florida, Texas and other states have introduced bills this year that would extend driving privileges to undocumented immigrants. Some of those states already allow the FBI to scan driver's license photos, while others, such as Florida and New York, are negotiating with the FBI over access, according to the GAO.

"The state has told [undocumented immigrants], has encouraged them, to submit that information. To me, it's an insane breach of trust to then turn around and allow ICE access to that," said Clare Garvie, a senior associate with the Georgetown Law center who led the research.

An ICE spokesman declined to answer questions about how the agency uses facial-recognition searches, saying its "investigative techniques are generally considered law-enforcement sensitive."

Asked to comment, the FBI referred *The Post* to the congressional testimony last month of Deputy Assistant Director Kimberly Del Greco, who said that facial-recognition technology was critical "to preserve our nation's freedoms, ensure our lib-

erties are protected, and preserve our security." The agency has said in the past that while facial-recognition searches can provide helpful leads, agents are expected to verify the findings and secure definitive proof before pursuing arrests or criminal charges.

Twenty-one states, including Texas and Pennsylvania, plus the District of Columbia, allow Federal agencies such as the FBI to scan driver's license photos, GAO records show. The agreements stipulate some rules for the searches, including that each must be relevant to a criminal investigation.

The FBI's facial-recognition search has access to local, state and Federal databases containing more than 641 million face photos, a GAO director said last month. But the agency provides little information about when the searches are used, who is targeted and how often searches return false matches.

The FBI said its system is 86 percent accurate at finding the right person if a search is able to generate a list of 50 possible matches, according to the GAO. But the FBI has not tested its system's accuracy under conditions that are closer to normal, such as when a facial search returns only a few possible matches.

Civil rights advocates have said the inaccuracies of facial recognition pose a heightened danger of misidentification and false arrests. The software's precision is highly dependent on a number of factors, including the lighting of a subject's face and the quality of the image, and research has shown that the technology performs less accurately on people with darker skin.

"The public doesn't have a way of controlling what information the government has on them," said Jacinta González, a senior organizer for the advocacy group Mijente who was particularly concerned about how ICE and other agencies could use the scans to track down immigrants. "And now there's this rapidly advancing technology, with very few guidelines and protections for people, putting all of this information at their fingertips in a very scary way."

The records, which include thousands of emails and official documents from Federal agencies, as well as Utah, Vermont and Washington State, show how easy it is for a Federal investigator to tap into an individual State DMV's database. While some of the driver photo searches were made on the strength of Federal subpoenas or court orders, many requests for searches involved nothing more than an email to a DMV official with the target's "probe photo" attached. The official would then search the driver's license database and provide details of any possible matches.

The search capability was offered not just to help identify criminal suspects, but also to detect possible witnesses, victims, bodies, and innocent bystanders and other people not charged with crimes.

Utah's DMV database was the subject of nearly 2,000 facial-recognition searches from outside law enforcement agencies between 2015 and 2017—sometimes dozens of searches a day, the records show. One document from Utah's Statewide Information & Analysis Center coached officers on how to make facial-recognition requests; offered four tips for better facial photographs ("lighting, distance, angle, eyes"); and said the database included "over 5 million Utah driver's license & state identification card photos," about 2 million more than the state's population. State officials did not respond to requests for comment.

Many of the requests for searches in Utah came from local police forces across the country seeking to find suspects who may have traveled to the state, but roughly half the searches came from Federal agents, according to a log of the searches. The records do not provide suspect names or say whether cases ended in arrests or convictions.

Washington state's Department of Licensing said that its "facial recognition system is designed to be an accurate, non-obtrusive fraud detection tool" and that the agency does not share use of the system with law enforcement unless compelled by a court order.

Vermont officials said they stopped using facial-recognition software in 2017. That year, a local chapter of the American Civil Liberties Union revealed records showing that the state DMV had been conducting the searches in violation of a state law that banned technology involving "the use of biometric identifiers." The state's Governor and attorney general came out against the face-scanning software, citing a need to balance public safety with residents' privacy rights.

In the years before the ban, the records show, Vermont officials ran a number of face scans on driver's license photos at the request of ICE agents. Investigators from a number of Federal and local agencies emailed the state's DMV with facial-recognition search requests as they pursued people accused of overstaying their visas, providing false information, stealing from stores or, in at least one case, being part of a "suspicious circumstance."

The officers in some emails would provide descriptions of their targets: One was dubbed a "gypsy . . . scamming elderly people for money," while another was said

to have "VERY LARGE PROTRUDING EARS." In others, DMV officials talked about the face-scanning tool as if it were the kind of awe-inspiring technical marvel most often seen on prime-time cop shows.

In one 2014 email, a police officer in the town of Manchester, Vt., asked a DMV official to scan for a man caught on video "brazenly" stealing. The official forwarded the email to a colleague with a made-for-TV flourish, writing, "Can we play NCIS for this officer?"

LETTER FROM TODD HAUPTLI, AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES

July 9, 2019.

The Honorable BENNIE THOMPSON,
Chairman, House Homeland Security Committee, Washington, DC 20515.

The Honorable MIKE ROGERS,
Ranking Member, House Homeland Security Committee, Washington, DC 20515.

DEAR CHAIRMAN THOMPSON AND RANKING MEMBER ROGERS: As experiences at airports across the country and the world illustrate, biometric technology holds tremendous promise in enhancing security and efficiency in the aviation environment. While airport executives are encouraged by the promise of biometrics and look forward to their further utilization, we recognize that there are legitimate privacy and civil right concerns that must be addressed before these technologies are deployed more widely. We look forward to working with the Committee and the Department of Homeland Security (DHS) to ensure that the proper regulatory framework and safeguards are in place to protect citizens' rights as these technologies are utilized to achieve worthy objectives.

As you know, many airport facilities across the country are already experiencing significant strain with passenger traffic at record levels. The situation is likely to become increasingly more challenging as airport facilities age and as domestic and international passenger levels continue to increase. International passenger traffic is growing at 5–6 percent at U.S. airports and domestic growth is nearing 5 percent, with some facilities seeing growth well beyond those annual averages. International air travel is projected to double over the next 20 years according to the International Air Transportation Association (IATA).

While there are clear economic benefits that accompany these increases in passengers, airport facilities—many of which are decades old—cannot keep pace with current growth. Similarly, our Federal partners at both U.S. Customs and Border Protection and the Transportation Security Administration will, undoubtedly, have significant difficulties handling record passenger volumes efficiently and effectively at current staffing levels, leading to growing wait times at checkpoints and in other processing queues.

In our view, innovation holds the key to improving the efficiency of the travelers' journey and reducing growing lines, which themselves pose a security challenge. Wider adoption of biometric technology at our borders and security checkpoints is one way that airports, airlines, and the Federal Government can more seamlessly handle expected passenger growth. Biometrics, including facial recognition, have the potential to enhance security and efficiency without compromising important civil liberties provided that their utilization is coupled with robust privacy and data protections for travelers and the ability for American citizens to opt out of using biometric technology in favor of the traditional screening process at an airport.

Additionally, as Federal budgets are tightening, we are concerned that DHS may shift the responsibility for acquiring these technologies onto airports at a time when State and local budgets are also constricting. This could lead to a bifurcated system in which certain airports or airlines have the financial resources to procure these biometric technologies and others do not, resulting in different protocols being used at different airports in the United States. We are already seeing the Department depend heavily on public-private partnerships to fund inherently governmental responsibilities for the screening and processing of passengers. Security cannot and should not become an area of "haves" and "have nots" at the nation's airports.

AAAE and our members would welcome the opportunity to discuss potential uses and security benefits of biometric and facial recognition technologies in the airport environment as you contemplate further Committee action in this area. We sincerely appreciate your consideration of our views and the need to innovate in order to address growing passenger volumes at our airports while maintaining the highest levels of security.

Sincerely,

TODD HAUPTLI,
President and CEO.

STATEMENT OF THE INTERNATIONAL BIOMETRICS + IDENTITY ASSOCIATION

July 9, 2019.

The Honorable BENNIE THOMPSON,
Chairman, Committee on Homeland Security, U.S. House of Representatives, 2466 Rayburn House Office Building, Washington, DC 20515.

The Honorable MIKE ROGERS,
Ranking Member, Committee on Homeland Security, U.S. House of Representatives, 2184 Rayburn House Office Building, Washington, DC 20515.

DEAR CHAIRMAN THOMPSON AND RANKING MEMBER ROGERS: On behalf of the International Biometrics + Identity Association, I am writing to express our gratitude for your support over the past decade for the use of biometrics by DHS, and especially CBP for its US–VISIT Entry Exit program. Through your efforts, CBP has come a long way in implementing biometrics to enhance the security of air travel, limit identification fraud, help address the visa overstay issue, and, at the same time, facilitate air travel.

A heated debate is now surrounding the emergence of facial recognition for use by CBP, TSA, and other DHS programs.

IBIA appreciates the opportunity to provide the following information about the performance of facial recognition algorithms that has not come out in the public hearings. The data that we are providing comes directly from NIST, the recognized global premier testing entity.

IBIA acknowledges that many people have concerns about privacy that are rooted in moral and political philosophies. These are matters of opinion on which reasonable people may disagree and should be resolved in the public sphere.

IBIA's objective is to provide facts that can help to inform the debate and conversations about facial recognition, facts that have not been properly aired to date. This is foundational for good legislation. We look to this Committee to help bring out the facts to ensure a full debate on the issues open to all stakeholders and relevant information.

Much of the debate has centered around the view that the algorithms are "biased" and "discriminatory". These words are semantically loaded and imply intent. Facial recognition is performed by a machine and machines have no intent.

ATTACHMENT.—INTERNATIONAL BIOMETRICS + IDENTITY ASSOCIATION

UNDERSTANDING THE PERFORMANCE OF FACIAL RECOGNITION ALGORITHMS

The International Biometrics + Identity Association (IBIA) is the leading voice for the biometrics and identity technology industry. It advances the transparent and secure use of these technologies to confirm human identity in our physical and digital worlds. #identitymatters

UNDERSTANDING THE PERFORMANCE OF FACIAL RECOGNITION ALGORITHMS

Executive Summary

This paper addresses the performance of facial recognition algorithms, an issue that has emerged as a major point of contention during the current policy debates about the use and limits of facial recognition.

The thrust of the argument to limit the use of facial recognition is that the technology is not yet ready for prime time. The primary arguments are that facial recognition algorithms are basically too imperfect because they are "discriminatory" against people with dark skin tones and display low levels of matching performance.

The purposes of this paper are to:

- Demonstrate these performance arguments are not supported by the evidence documented in recent National Institute of Standards and Technology (NIST) testing, the world's premier standards and testing body. NIST shows stunningly high levels of accuracy and clear superiority of the technology compared to human recognition systems, both in terms of accuracy rates and performance across a range of skin tones. This is supported by the latest academic research conducted by a group of the preeminent scholars on facial recognition.
- Explain the factors that affect the performance differences of facial recognition algorithms, including the application, the rest of the system, variations in quality of the algorithms.
- Summarize the many benefits of facial recognition.
- Highlight the challenges in the use of facial recognition that remain and address the work in progress to further improve the technology.

The field of research today known as Artificial Intelligence traces its origins to a workshop at Dartmouth College in 1956. Attendees became the founders and lead-

ers of the field and were, with the benefit of hindsight, unrealistic about the likely course of progress. For example, Herbert Simon predicted, "machines will be capable, within 20 years, of doing any work a man can do." Marvin Minsky agreed, writing "within a generation . . . the problem of creating 'artificial intelligence' will substantially be solved." What AI research has delivered are highly specialized tools which approximate or improve upon human performance in narrow areas, yet exhibit no generalized behavior that humans would recognize as intelligence. Deep Learning is another such term that implies an on-going process similar to that employed by humans; whereas what actually occurs is a highly sophisticated, one time, training on substantial amounts of carefully annotated data. Thereafter the system works well with information similar to the training data but does not adapt to new data until a subsequent training period.

Let's Stop Using Semantically Loaded Terms like "Discriminatory"

- Let's dispense with this term so we can focus on the essential facts about performance of facial recognition systems, including accuracy and systemic errors, instead of extraneous and emotional issues.
- "Discriminatory" is a semantically loaded term because it implies intent.
- However, facial recognition is performed by a machine, and machines have no intent.
- The argument that algorithm developers exhibit racial/gender blindness producing algorithms that perform less effectively for other than white males is not supported by the facts.
- NIST has active test and analysis effort to assess this issue.
- Recent (12 April 2019) results for verification algorithms (i.e. 1:1 search) show the top 20 performing algorithms, with elapsed time between images from 2–16 years, are most effective for blacks with black females often the most accurate.
- The test results for identification (i.e. 1:N search) are expected during 2Q 2019.
- The most appropriate composition of test datasets, to insure effective testing, is still somewhat of an unsettled issue.

Cost of new dataset development for effective large-scale testing is a significant issue, beyond the resources of all but government and the largest companies. It may be feasible to continue to employ existing facial recognition datasets, by recharacterizing their metadata to more accurately reflect subject demographics, once there is consensus on what changes, if any, are needed.

Performance Differences of Algorithms

- All algorithms have some performance differences across different demographic groups, genders, and age cohorts.
- These differences are being addressed and there has been rapid improvement, which is on-going.
- For verification applications (fraud detection, access control, etc.), in the latest NIST testing, the top performing algorithms are more accurate with black males and females than with whites and have less than 1 percent false non-match rates for all groups at 0.1 percent false match rate.
- For investigative applications, progress has been dramatic with a major update report expected from NIST during the 2d quarter of 2019.

Facial Recognition and Facial Classification are Different and Should Not Be Confused

- Face recognition seeks to identify an individual from their face image.
- Facial classification seeks to classify a face by estimating, for example, gender, age, or race.
- The algorithms are built and trained separately.
- The process of classification estimation involves one image, while facial recognition involves comparison of pairs.
- An MIT study, which is a large part of the "facial recognition is biased narrative"; only examined facial classification, specifically for gender.
- A joint FIT/Notre Dame study provides a more complete and accurate view, as do the NIST tests.

Algorithms Are Just Part of a Facial Recognition System

- The performance of a facial recognition system depends on a number of factors; the algorithm is one such factor. The camera, its resolution, positioning, distance, and lighting set an upper limit on performance. Subject pose and expression can also influence performance.

- Camera resolution and distance matter; humans require about 25 pixels per meter resolution to detect the presence of humans, but can recognize motion at lower resolutions.
- Ambient or artificial lighting has an enormous impact on system performance.
- In other words, all the components of the facial recognition system must perform properly, in addition to using a high-performance algorithm, and these elements can be adjusted easily.
- Knowing all this, some facial recognition applications employ human facial examiners who make the final match/no match decision after the facial matching algorithm selects a list of potential matches; they use applications specifically designed for facial examinations.

The Application Matters

- Facial verification and facial identification systems, until quite recently, have been designed to match portrait style (mugshot, driver license, visa, passport) images.
- With good lighting, pose, and expression control, performance can be stunningly good and good mugshot accuracy conforms to photography standards adopted by NIST for the FBI further developed by ISO.
- Matching of "in the wild" images (a reference to image quality—candid, unposed, not portrait-style images) has matured dramatically in the past 5 years, with verification accuracy of top algorithms now at 99 percent. An update on investigation applications is expected to show comparable progress and further maturation is expected in the near term.

Some algorithms are much better than others, as in everything else. In golf, there is Tiger Woods and then there is the rest of us.

Not all Algorithms are Alike

- Market entry is relatively easy and the number of algorithm providers has expanded from about 10 in 2010 to about 100 today, with many offering multiple algorithms.
- Some algorithms are much better than others, as would be expected. Objective testing like that performed by NIST reveals the differences.
- Algorithm performance for a selfie, social media, or a commodity web camera is considerably different from an algorithm used for security or law enforcement applications.

NIST Has Tested More Than 170 FR Algorithms, with Wide Variations in Performance Observed

- Six (6) algorithms are less accurate than a coin toss.
- Most are more accurate than human observers, including those trained and employed to do recognition.
- The top performing algorithms are much better performing than humans.
- Many algorithms match blacks more accurately than whites.
- Algorithm matching of females is frequently less accurate than males.
- Algorithm performance is less accurate for most applications involving children.
- The application makes a difference.
- Portrait style 1:N and 1:1 matching is extraordinarily accurate (considerably more accurate than fingerprint technology circa mid-2000's when FBI went to partial "lights out" fingerprint matching).

Nothing is perfect and no system performs perfectly. The real question is whether automated facial recognition is better than the current systems. And under this criterion, data clearly demonstrates superior performance of automated facial recognition.

- In the wild ("candid, unposed, non-portrait images"), matching is less accurate but quite suitable for lead generation, typically with stalled investigations.
- Likewise, matching is less accurate for poor quality images.
- Notwithstanding exceptional algorithm accuracy, validation has not been performed to allow "lights out" use of facial recognition technology when there are potential adverse consequences to the subjects. Human review is required.
- Algorithms are not commoditized as performance varies greatly, from the best identifying 99.4 percent of individuals in a gallery of 12 million subjects to below 40 percent for the worst.

Demand for Perfection of Algorithms is Not a Performance Standard for the Real World

- No system—or human—performs perfectly.

- The real question is whether automated facial recognition is better than other systems or humans. And under this criterion, data clearly demonstrate superior performance of automated facial recognition.
- For family, friends, professional acquaintances, and celebrities, human recognition works well.
- For unfamiliar persons, few individuals perform well at face recognition or matching.
- Skilled passport examiners are only about 80 percent accurate when unaided by automation.
- The top performing algorithms outperform the mean performance of all human groups including skilled forensic face examiners with unlimited time and the best automated tools; (although a few humans in the more skilled groups outperform circa 2017 top algorithms).
- Machines can memorize millions of faces, and humans only thousands, enabling machines to do things unaided that humans cannot, including to:
  - Identify missing children who do not know their names.
  - Identify exploited children in dark web pornography.
  - Identify disoriented adults (e.g. with amnesia, Alzheimer's).
  - Flag likely driver license application fraud for human review.
  - Identify likely Visa fraud for human review.
  - Identify likely Passport fraud for human review.
  - Provide leads for further investigation when a surveillance photo is the only information.
  - Detect border (and other) fraudulent use of stolen identity documents.

People are Comfortable with Face Recognition

- Following the iPhone X introduction on November 3, 2017, tens of millions of Americans have become familiar and entirely satisfied with facial recognition technology for personal use.
- The 2019 Center for Data Innovation public opinion survey found that only 1 in 4 Americans think the government should strictly limit the use of facial recognition technology.
- The technology is widely used worldwide, and adoption is growing.
- DHS pilot projects at several airports, dispensing with boarding passes and ID cards in favor of facial recognition for international flights, have been enthusiastically greeted by the traveling public.
- Frequent international travelers already hope for domestic adoption.
- Technology advancement is inexorable, and each generation has the responsibility to decide how to balance the benefits of new technology with privacy and appropriate uses.

The IBIA is the leading voice for the biometrics and identity technology industry. It advances the transparent and secure use of these technologies to confirm human identity in our physical and digital worlds. Visit us at *www.ibia.org*.

LETTER SUBMITTED BY CHAIRMAN BENNIE G. THOMPSON

July 9, 2019.

The Honorable BENNIE THOMPSON,
Chairman, Committee on Homeland Security, 310 Cannon House Office Building, Washington, DC 20515.

The Honorable MIKE ROGERS,
Ranking Member, Committee on Homeland Security, 310 Cannon House Office Building, Washington, DC 20515.

RE: The Suspension of Face Recognition Technology Use by the Department of Homeland Security

DEAR CHAIRMAN THOMPSON AND RANKING MEMBER ROGERS: The undersigned organizations, which are dedicated to preserving privacy, civil liberties, and civil rights, write to urge you to immediately suspend the Department of Homeland Security's (DHS) use of face recognition technology on the general public.

The use of face recognition technology by the DHS poses serious risks to privacy and civil liberties, threatens immigrants, broadly impacts American citizens, and has been implemented without proper safeguards in place or explicit congressional approval. The technology is being deployed today by authoritarian governments as a tool to suppress speech and monitor critics, minorities, and everyday citizens. Congress should not permit the continued use of face recognition in the United States absent safeguards to prevent such abuses.

Moreover, the extraordinary breach of the images of travelers' faces and license plates, surveillance-equipment schematics and sensitive contracting documents by a CBP contractor has made clear that these programs are creating new risks to the privacy and security of Americans.[1] Through carelessly managed programs, DHS itself created new security threats. It would be irresponsible for DHS to move forward with face recognition programs that collect massive amounts of sensitive data until a thorough investigation of this incident is completed and the agency demonstrates that it can fully safeguard its systems.

DHS's Use of Face Recognition Technology

DHS is in the process of integrating and expanding the agency's use of face recognition technology through various programs of its subcomponents. DHS's use of face recognition will affect millions of individuals, who will lack the protections needed against a powerfully invasive surveillance tool.

Customs and Border Protection

The broadest current use of face recognition technology is the Customs and Border Protection's Biometric Entry-Exit program. Without legal authority or the opportunity for public comment, the U.S. Customs and Border Protection (CBP) has broadly deployed facial recognition technology at U.S. airports to all travelers, including U.S. citizens. The agency plans to "incrementally deploy biometric capabilities across all modes of travel—air, sea, and land—by fiscal year 2025."[2]

CBP uses flight manifests and photographs obtained from the State Department to create "galleries" to match with photos captured at international airports.[3] "If CBP does not have access to advance passenger information, such as for pedestrians or privately-owned vehicles at land ports of entry, CBP will build galleries using photographs of 'frequent' crossers for that specific port of entry[.]"[4] CBP uses its own equipment as well as that of private firms, other government agencies, and foreign governments to capture face images.[5] Yet, there are no formal rules restricting the use of the photos captured by non-CBP owned equipment.[6]

The steady implementation of CBP's biometric entry-exit program in airports across the country has been widely reported.[7] The program affects a significantly large group of U.S. citizens traveling in and out of the country. At the Atlanta Hartsfield-Jackson International Airport alone, "[a]bout 25,000 passengers move through the terminal each week" and the majority of those passengers are subject to facial recognition.[8] Further, "CBP hopes to have facial recognition boarding at all US airports serving international flights within 3 or 4 years."[9]

---

[1] Drew Harwell, *Hacked documents reveal sensitive details of expanding border surveillance,* Wash. Post (June 21), *https://www.washingtonpost.com/technology/2019/06/21/hacked-documents-reveal-sensitive-details-expanding-border-surveillance/*.

[2] U.S. Dep't of Homeland Sec., Office of Inspector Gen., OIG–18–80, Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide, 7 (Sept. 21, 2018), *https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf* [hereinafter OIG Report].

[3] Id.

[4] U.S. Dep't of Homeland Sec., U.S. Customs and Border Protection, DHS/CBP/PIA–0056, Privacy Impact Assessment for the Traveler Verification Service, 5 (Nov. 14, 2018) *https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018__2.pdf* [hereinafter TVS Nov. 2018 PIA].

[5] Id. at 7–8.

[6] *See Memorandum of Understanding Between and Among U.S. Customs and Border Protection and [REDACTED] and [REDACTED] Regarding [REDACTED] Biometric Pilot Project at [REDACTED]* (June 2017), *https://epic.org/foia/dhs/cbp/biometric-entry-exit/MOU-Biometric-Pilot-Project.pdf.*

[7] See e.g., Bart Jansen, *CBP: Orlando is First U.S. Airport to Scan Faces of All International Travelers,* USA Today (June 21, 2018), *https://www.usatoday.com/story/travel/flights/todayinthesky/2018/06/2/orlando-international-airport-scan-faces-u-s-citizens/722643002/;* Lori Aratani, *Officials Unveil New Facial Recognition System at Dulles International Airport,* Wash. Post (Sept. 7, 2018), *https://www.washingtonpost.com/transportation/2018/09/06/officials-unveil-new-facial-recognition-system-dulles-international-airport/;* Gregory Wallace, *Instead of the Boarding Pass, Bring Your Smile to the Airport,* CNN (Sept. 10, 2018), *https://www.cnn.com/travel/article/cbp-facial-recognition/index.html;* Jack Stewart, *Creepy or Not, Face Scans Are Speeding Up Airport Security,* Wired (Nov. 21, 2018), *https://www.wired.com/story/airport-security-biometrics-face-scanning/;*.

[8] Lori Aratani, *Your Face is Your Boarding Pass at this Airport,* Wash. Post (Dec. 4, 2018), *https://www.washingtonpost.com/nation/2018/12/04/your-face-is-your-boarding-pass-this-airport/*.

[9] Thom Patterson, *US Airport Opens First Fully Biometric Terminal,* CNN (Dec. 3, 2018), *https://www.cnn.com/travel/article/atlanta-airport-first-us-biometric-terminal-facial-recognition/index.html.*

The Biometric Entry-Exit program is flawed. A report on iris and facial recognition technologies at a southern land border found that the technologies did not perform operational matching at a "satisfactory" level.[10] A DHS Office of the Inspector General ("IG") report found that CBP's Biometric Entry-Exit program suffered from technical and operational challenges. The IG report also found that CBP could not "produce biometric matches consistently for individuals in certain passenger groups" with the lowest biometric confirmation rate being for U.S. citizens.[11] Moreover, several reports and studies have noted that face recognition algorithms are often less accurate on certain sub-groups, including women and people with darker skin pigmentation.[12]

Americans returning to the United States have also found it difficult to opt out of the facial recognition screening, which is their legal right.[13] Travelers routinely report on burdensome procedures intended to compel individuals to undergo facial recognition even if that is not their choice.[14] Additionally, CBP has not undergone formal rulemaking addressing how information collected will be used, disclosed, and retained, and what remedies will exist in cases where individuals are adversely impacted by the use of the technology.

These concerns are further amplified given that CBP uses face recognition technology for purposes that extend far beyond simply verifying whether someone purportedly matches the photograph on their travel document. CBP plans to use the facial recognition to search biometric watch lists—raising questions about how such lists will be compiled and whether they will be the predicate for additional immigration and law enforcement activities.[15] The data from the Biometric Entry-Exit program will also be broadly accessible within DHS with the Coast Guard, Transportation Security Administration (TSA), and Immigration and Customs Enforcement (ICE) all having access to the data.[16]

Transportation Security Administration

The TSA has plans to expand the use of face recognition to all domestic travelers.[17] The TSA Biometric Roadmap envisions the use of face recognition for booking, check-in, bag drop, the security line, access to an airport lounge, and boarding.[18] TSA states it "will pursue a system architecture that promotes data sharing to maximize biometric adoption throughout the passenger base and across the aviation security touchpoints of the passenger experience."[19]

Similar to CBP, ISA has not undergone rulemaking clarifying how information will be collected, used, or retained. However, TSA's biometric roadmap suggests that its system will be interoperable with CBP, and thus may be utilized for other immigration and law enforcement activities.

Immigration and Customs Enforcement

Recent news reports show that ICE has expanded the agency's deployment and use of face recognition systems. Public records covered by the press this week show

---

[10] U.S. Customs and Border Protection, *Southern Border Pedestrian Field Test Summary Report,* 8 (Dec. 2016), *https://epic.org/foia/dhs/cbp/biometric-entry-exit/Southern-Border-Pedestrian-Field-Test-Report.pdf.*

[11] OIG Report at 19.

[12] See, e.g., Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77–91 (2018), *http://proceedings.mlr.press/v8l/buolamwini18a/buolamwini18a.pdf.*

[13] See Zack Whittaker, *Yes, Americans can opt-out of airport facial recognition—here's how,* Tech Crunch, *https://techcrunch.com/2019/05/13/americans-opt-out-facial-recognition-airport/ ;* Allie Funk, *I Opted Out of Facial Recognition at the Airport—It Wasn't Easy,* Wired, July 2, 2019, *https ://www.wired.com/story/opt-out-of-facial-recognition-at-the-airport/.*

[14] Allie Funk, *I Opted Out of Facial Recognition at the Airport—It Wasn't Easy,* Wired, July 2, 2019, *https://www.wired.com/story/opt-out-of-facial-recognition-at-the-airport/.*

[15] U.S. Department of Homeland Security U.S. Customs and Border Protection, *Biometric Entry-Exit Program Concept of Operations, 000039 (June 27, 2017), https://epic.org/foia/dhs/cbp/biometric-entry-exit/CBP-Biometric-Entry-Exit-Concept-of-Operations.pdf.*

[16] See U.S. Department of Homeland Security U.S. Customs and Border Protection, Biometric Entry-Exit Program Concept of Operations 000063 (June 27, 2017), *https://epic.org/foia/dhs/cbp/biometric-entry-exit/Concept-of-Operations.pdf;* see also U.S. Department of Homeland Security, Capability Analysis Study Plan for Biometric Ently Exit 000160–000161, *https://epic.org/foia/dhs/cbp/biometric-entry-exit/Capability-Analysis-Study-Plan.pdf.*

[17] Transportation Security Administration, *TSA Biometrics Roadmap* (Sept. 2018), *https://www.tsa.gov/sites/default/files/tsa__biometrics__roadmap.pdf.*

[18] Id. at 18.

[19] Id. at 17.

that ICE has been sending facial recognition requests to State DMVs for years.[20] As a result, millions of innocent State residents have had their faces scanned by ICE without notice or consent. Internal documents also suggest that ICE plans to leverage CBP's biometric entry-exit system to identify and search for information regarding non-citizens encountered during enforcement activities.[21]

In addition, last year, Amazon marketed the company's facial recognition service "Rekognition" to ICE for border control.[22] A test of Amazon's face recognition software resulted in Amazon's technology falsely matching 28 Members of Congress to mugshots and other tests have similarly found the technology to be less accurate on individuals with darker skin pigmentations.[23]

There is a lack of public information on how ICE might use the face recognition capabilities implemented as part of the Biometric Entry-Exit program, ICE's current use of face recognition technology, and whether the agency intends to deploy other face recognition capabilities. There is a serious risk that ICE could deploy face recognition for purposes of indiscriminate immigration enforcement and use the technology, despite its record of error, as a pretext for aggressive questioning and harassment of immigrants—including those lawfully present in the United States.

Secret Service

The U.S. Secret Service is testing the use of face recognition technology to identify people in the public spaces in and around the White House.[24] The spaces around the White House are regularly used for First Amendment-protected protests and demonstrations. The possible use of face recognition to identify individuals near the White House raises serious First Amendment issues and threatens to chill speech.

DHS'S USE OF FACE RECOGNITION LACKS PROPER SAFEGUARDS AND POSE SUBSTANTIAL RISKS

Use of face recognition poses a unique threat to Constitutional rights.—Participation in society necessarily exposes one's images in public spaces. But ubiquitous and near-effortless identification eliminates the individual's ability to control the disclosure of their identities to others and poses a special risk to the First Amendment rights of free association and free expression. The proposed plans by DHS risk creating a world where individuals are forced to submit to face recognition surveillance simply to exercise their right to travel.

The aggregation of biometric data for the use of face recognition and the broad dissemination of this data poses cybersecurity risks and increases the risk of a data breach.—Indeed, a CBP vendor who had collected images of travelers along with license plate reader data and other sensitive information was subject to a recent data breach.[25]

Face recognition technology will disproportionately impact already marginalized groups. Studies have shown that facial recognition has significantly higher error rates for darker-skinned individuals.[26] It is unacceptable for DHS to implement a technology with a documented racial bias without proving that such a bias has been eliminated. Moreover, use of face recognition for immigration enforcement raises further risks of a disproportionate impact on already marginalized groups.

The agency continues to expand the use of face recognition beyond what was ever authorized by Congress.—In fact, the Biometric Entry-Exit program itself is an example of mission creep. The program leverages the photos provided by passport ap-

---

[20] Drew Harwell, *FBI, ICE find State driver's license photos are a gold mine for facial-recognition searches,* Wash. Post (July 7, 2019), *https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/*.

[21] See U.S. Department of Homeland Security U.S. Customs and Border Protection, *Biometric Entry-Exit Program: Concept of Operations, 000063 (June 2017), https://epic.org/foia/dhs/cbp/biometric-entry-exit/CBP-Biometric-Entry-Exit-Concept-of-Operations.pdf*.

[22] Drew Harwell, *Amazon met with ICE officials over facial-recognition system that could identify immigrants,* Wash. Post (Oct. 23, 2018), *https://www.washingtonpost.com/technology/2018/10/23/amazon-met-with-ice-officials-over-facial-recognition-system-that-could-identify-immigrants/*.

[23] Natasha Singer, *Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says,* N.Y. Times (July 26, 2018), *https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-Congress.html*.

[24] USSS PIA at 1, *https://www.dhs.gov/sites/default/files/publications/privacy-pia-usss-frp-november2018.pdf*.

[25] Drew Harwell, *Hacked documents reveal sensitive details of expanding border surveillance,* Wash. Post (June 21), *https://www.washingtonpost.com/technology/2019/06/21/hacked-documents-reveal-sensitive-details-expanding-border-surveillance/*.

[26] Joy Buolamwini (MIT Media Lab) and Timnit Gebru (Microsoft Research), *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* (2018), *http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf*.

plicants to the State Department, who provided the photos for the specific purpose of obtaining a passport, only to see those photos used in conjunction with face recognition technology to create a digital ID. Additionally, the State Department then disclosed the biometric data to other agencies, including DHS, and there was nothing a passport holder could do to prevent the disclosure. And, there is nothing an individual could do to stop DHS from further disseminating their biometric data.

DHS's use of face recognition lacks the safeguards needed to prevent overcollection, overly broad uses, wide-spread dissemination, and unnecessarily long retention.—Moreover, DHS has failed to show that less invasive alternatives could not be used. DHS has moved forward with face recognition with a focus on justifying its implementation and not a focus on whether, given the risks, the technology should be implemented.

CONCLUSION

Face recognition is an especially dangerous technology in need of strict limits on its use, robust transparency, oversight, and accountability. It is imperative that Congress suspend DHS's use of face recognition until Congress fully debates what, if any, proposed uses should move forward.

If you have questions, please contact Jeramie D. Scott, EPIC Senior Counsel, atjscott@epic.org.

Sincerely,

ACCESS NOW
ACLU
AMERICAN-ARAB ANTI-DISCRIMINATION COMMITTEE (ADC)
ALGORITHMIC JUSTICE LEAGUE
CENTER FOR DEMOCRACY & TECHNOLOGY
CENTER FOR DIGITAL DEMOCRACY
CENTER ON PRIVACY & TECHNOLOGY AT GEORGETOWN LAW
CONSTITUTIONAL ALLIANCE
CONSUMER ACTION
CONSUMER FEDERATION OF AMERICA
COUNCIL ON AMERICAN-ISLAMIC RELATIONS (CAIR)
CYBER PRIVACY PROJECT
DEFENDING RIGHTS & DISSENT
DEMAND PROGRESS
ELECTRONIC FRONTIER FOUNDATION
ELECTRONIC PRIVACY INFORMATION CENTER
FIGHT FOR THE FUTURE
FREE PRESS ACTION
FREEDOM WORKS
GOVERNMENT ACCOUNTABILITY PROJECT
IMMIGRANT RIGHTS CLINIC
OF THE UNIVERSITY OF CALIFORNIA AT IRVINE SCHOOL OF LAW
LIBERTY COALITION
MEDIAJUSTICE
MIJENTE
NATIONAL IMMIGRATION LAW CENTER
NATIONAL WORKRIGHTS INSTITUTE
NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE
OPEN MIC (OPEN MEDIA AND INFORMATION COMPANIES INITIATIVE)
OPEN THEGOVERNMENT
PATIENT PRIVACY RIGHTS
PRIVACY TIMES
PROJECT ON GOVERNMENT OVERSIGHT
PROJECT SOUTH
PUBLIC CITIZEN
RESTORE THE FOURTH
TECHFREEDOM
TRI-STATE COALITION FOR RESPONSIBLE INVESTMENT

Chairman THOMPSON. The Chair now recognizes the Ranking Member of the full committee, the gentleman from Alabama, Mr. Rogers, for an opening statement.

Mr. ROGERS. Thank you, Mr. Chairman. Biometric technologies have the potential to improve security, facilitate travel, and better enforce our immigration laws. These technologies range from facial

recognition to fingerprints to DNA. Each of these methods present unique privacy considerations but also clear security benefits. Not only does Federal law authorize DHS to use biometrics to verify identities, it requires CBP to collect biometric entry and exit data for all foreign nationals. This requirement has been a long-standing, bipartisan mandate. Recent technological advancements have finally made it possible. DHS's primary focus is facial recognition at TSA and CBP checkpoints, where travelers are already providing IDs to Government employees. TSOs and CBP agents can review several hundred IDs in a single shift. As a result, fatigue and human error allow people with fake IDs to slip into our country every day. Automating this process with biometric technology will improve transportation security.

CBP and TSA have done their homework on these checkpoint pilots and are working to build accurate, effective, and secure systems. DHS should continue to collaborate with experts at NIST to ensure they are using accurate algorithms to power these systems.

Biometric systems advance DHS's mission beyond transportation security. ICE recently conducted a rapid DNA pilot program to verify family ties on the Southwest Border. A 90-minute test can replace hours of interviews and document review. This short pilot found a disturbing number of cases were men who claimed to be the biological parent of a child quickly changed their story when asked to submit DNA. The technology does not store DNA in a central database, and each machine can be purged daily.

Amid the humanitarian crisis on our border, we should be looking at things like rapid DNA to protect children from abuse by smugglers who rent them as a ticket into our country.

Additionally, we should be using biometrics to enforce our immigration laws. Recent reports have emphasized ICE and FBI's use of DMV photos to identify criminals. I do not believe that anyone has a reasonable expectation of privacy in a Government ID photo. Period. Police have long relied on photo books and manual photo reviews to identify suspects known as fugitives—or known fugitives.

Effective facial recognition technologies can improve law enforcement by ridding this process of bias and human error. Each of these examples use biometrics as a part of the process. Technology cannot and should not replace the officer's final judgment, but it can speed up the identity verification for millions of people every year.

Halting all Government biometric programs, as some of my colleagues suggest, is an easy way to avoid hard questions. Taking the easy way out of this issue will not increase the gap between technology and our ability to understand it. DHS should continue to consult with experts at NIST to develop clear public standards for Government biometric systems. DHS leadership should ensure that these biometric databases are secure and have clear privacy guidelines. Congress should continue to educate itself as we are today, about the way we can employ this technology responsibly. I thank you, Mr. Chairman. I yield back.

[The statement of Ranking Member Rogers follows:]

STATEMENT OF RANKING MEMBER MIKE ROGERS

Biometric technologies have the potential to improve security, facilitate travel, and better enforce our immigration laws.

These technologies range from facial recognition, to fingerprints, to DNA.

Each of these methods presents unique privacy considerations, but also clear security benefits.

Not only does Federal law authorize DHS to use biometrics to verify identities, it requires CBP to collect biometric entry and exit data for all foreign nationals. This requirement has been a long-standing bipartisan mandate. Recent technological advancements have finally made it possible.

DHS's primary focus is facial recognition at TSA and CBP checkpoints, where travelers are already providing IDs to Government employees.

TSOs and CBP Agents can review several hundred IDs in a single shift.

As a result, fatigue and human error allow people with fake IDs to slip into our country every day.

Automating this process with biometric technology will improve transportation security.

CBP and TSA have done their homework on these checkpoint pilots and are working to build accurate, effective, and secure systems.

DHS should continue to collaborate with experts at NIST to ensure they are using accurate algorithms to power these systems.

Biometric systems advance DHS's mission beyond transportation security.

ICE recently conducted a Rapid DNA pilot program to verify family ties on the Southwest Border.

A 90-minute test can replace hours of interviews and document review.

This short pilot found a disturbing number of cases where men, who claimed to be the biological parent of a child, quickly changed their story when asked to submit DNA.

The technology does not store DNA in a central database and each machine can be purged daily.

Amid the humanitarian crisis on our border we should be looking to things like Rapid DNA to protect children from abuse by smugglers who rent them as a ticket into our country.

Additionally, we should be using biometrics to enforce our immigration laws.

Recent reports have emphasized ICE and the FBI's use of State DMV photos to identify criminals.

I do not believe that anyone has a reasonable expectation of privacy in a Government ID photo. Period. Police have long relied on photo books and manual photo review to identify suspects and known fugitives.

Effective facial recognition technologies can improve law enforcement by ridding this process of bias and human error.

Each of these examples uses biometrics as one part of a process.

Technology cannot and should not replace an officer's final judgment. But it can speed up identity verification for millions of people every year.

Halting all Government biometric programs, as some of my colleagues suggest, is an easy way to avoid hard questions.

Taking the easy way out of this issue will only increase the gap between technology and our ability to understand it.

DHS should continue to consult with experts at NIST to develop clear public standards for Government biometric systems.

DHS leadership should ensure that its biometric databases are secure and have clear privacy guidelines.

And Congress should continue to educate itself, as we are today, about the way we can employ this technology responsibly.

Chairman THOMPSON. Thank you.

Other Members of the committee are reminded that, under the committee rules, opening statements may be submitted for the record.

I now welcome our panel of witnesses. Our first witness is Mr. John Wagner, deputy executive assistant commissioner at the U.S. Customs and Border Protection.

Next, we have Mr. Austin Gould, assistant administrator for requirements and capabilities analysis at the Transportation Security Administration.

Next, we have Mr. Joseph R. Di Pietro, the chief technology officer of the U.S. Secret Service.

Finally, we have Dr. Charles Romine, the director of the information technology laboratory at the Commerce Department's National Institute of Standards and Technology.

I look forward to hearing from you all today.

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. Chairman Thompson, Ranking Member Rogers, Members of the committee, thank you for the opportunity to testify before you today on behalf of U.S. Customs and Border Protection. I would like to begin with a few excerpts from the 9/11 Commission report.

When people travel internationally, they usually move through defined channels or portals. They may seek to acquire a passport. They may apply for a visa. They may stop at ticket counters, gates, and exit controls at airports and seaports. Upon arrival, they pass through inspection points. They may transit to another gate to get on an airplane. Each of these checkpoints or portals is a screening, a chance to establish that people are who they say they are and are seeking access for their stated purpose.

The job of protection is shared amongst these many defined checkpoints. By taking advantage of them all, we need not depend on any one point in the system to do the whole job. The challenge is to see the common problem across agencies and functions, and develop a conceptual framework and architecture for an effective screening system. Throughout Government and, indeed, in private enterprise, agencies, firms at the portals confront recurring judgments that balance security, efficiency, and civil liberties. These problems should be addressed systemically, not in an ad hoc, fragmented way. Like I mentioned, these are excerpts from the 9/11 Commission report.

Before CBP presented our current strategy, airlines, airports, private vendors, and Government agencies, including DHS were developing their own independent, biometric-based schemes. In other words, exactly what the 9/11 Commission warned against doing—an ad hoc, fragmented approach. CBP has developed a plan that includes other authorities and responsibilities in our mission set beyond just the biometric entry-exit mandate for foreign nationals. We saw the solution had to encompass the entire travel spectrum. We needed a solution that would also comport with the modernization and emerging biometric plans of airports, airlines, and cruise lines. Why? Well, because we don't have a transportation system

that allows the easy segmentation of only foreign visitors on international departures.

Previous DHS efforts failed for 10 years because they tried to create a stand-alone, stovepiped, unintegrated process. As we all know, those plans were cost-prohibitive, would create massive congestion, and there was significant opposition from the airlines and the travel industry. So, as a result, CBP developed a service that simply automates the manual, facial recognition process that goes on today when a traveler presents a passport to establish their identity.

To be clear, CBP is only comparing the picture taken against photos of previously provided by travelers to the U.S. Government for the purposes of international travel. This is not a surveillance program.

Since airlines and cruise lines are already required by statute to provide the biographic passport details of all travelers on international itineraries, CBP simply assembles a small gallery of photos of these expected travelers. These gallery photos are primarily from passports, visas, and previous international arrivals. A photo is taken and quickly searched against these distinct galleries, and thereby validating the biographic data that has already been vetted for National security and law enforcement concerns and corresponds to the traveler we all expect it to. We do not run the photo taken at the airport or seaport against any other databases or sources of information if it matches that pre-staged gallery photo.

If a traveler matches a U.S. passport, then the new photo taken is deleted. There is no need for us to keep it. U.S. citizens are clearly not part of the biometric entry-exit tracking system.

Now, recognizing there have been concerns raised over the inclusion of U.S. citizens, CBP has existing authorities and responsibilities to determine the citizenship and identity of all people traveling internationally. This is a U.S. Government responsibility, not the private sector. It is also unlawful for a U.S. citizen to travel internationally without a U.S. passport.

Now, generally, determination of U.S. citizenship is done by comparing the traveler against their passport. Again, we are simply automating and using a computer algorithm to enhance this manual facial recognition existing process. As we saw at Dulles Airport a few months ago, we had two travelers presenting U.S. passports claiming to be U.S. citizens. However, it was found that they were foreign nationals and imposters to these documents.

Now, as far as our partnerships with the industry stakeholders, CBP has developed a standard set of business requirements that our partners have all agreed to, if their camera is sending a photo to CBP. The business requirements clearly stipulate they cannot keep the photos. Going back to the ad hoc, fragmented approach mentioned earlier, our partners have voluntarily agreed to the CBP business requirements. This make a single, simple, consistent, transparent approach to the use of this technology for international travel.

CBP is already bound by and in compliance with existing privacy, technology, and data collection requirements found in the Privacy Act, the E-Government Act and the Homeland Security Act.

Our private-sector partners are basically signing on to these same requirements. We do recognize we can improve the public's understanding of these requirements and the opt-out provisions.

We have published a comprehensive, privacy-impact assessment, the required system of record notice for our databases, and rulemaking as commenced to put updates into the Federal regulations it is currently circulating within the Government.

In conclusion, we are solving a very difficult challenge: Biometric exit. We are solving it by focusing on improving the overall travel experience. We are building a tokenless, efficient, secure, international travel experience. Airlines and cruise lines have reported reduced boarding times and increased passenger satisfaction using this system. This system will allow us to build a world-class travel system in the United States. This will be the envy of the world as we try to keep pace with the record-breaking growth of international travel. So thank you for the opportunity to be here today, and I look forward to your questions.

[The prepared statement of Mr. Wagner follows:]

PREPARED STATEMENT OF JOHN P. WAGNER

JULY 10, 2019

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 (IATA),[1] the World Travel and Tourism Council,[2] and the Department of Commerce Travel and Tourism Advisory Board.[3] With air travel growing at 4.9 percent per year, and expected to double by 2031, and an increasingly complex threat posture, CBP must innovate and transform the current travel processes in order to handle this new volume without significant personnel and infrastructure investments. Facial comparison technology will enable CBP and travel industry stakeholders to position the U.S. travel system as best in class, which will in turn drive the continued growth in air travel volume.

As authorized in several statutes and regulations,[4] CBP is Congressionally-mandated to implement a biometric entry-exit system. Prior to the Consolidated and Further Continuing Appropriations Act of 2013 (Public Law 113–6), which transferred the biometric exit mission from the Department of Homeland Security (DHS) generally to CBP, the U.S. Government and the private sector were developing independent biometrics-based schemes. These varied, and often uncoordinated, investments relied on multiple biometrics and required complicated enrollment processes.[5] DHS, the Transportation Security Administration (TSA), legacy United States Visitor and Immigrant Status Indicator Technology, and several private-sector compa-

[1] *https://www.iata.org/pressroom/pr/Documents/resolution-one-id-agm–2019.pdf*.

[2] *https://www.wttc.org/about/media-centre/press-releases/press-releases/2019/we-must-act-and-assign-priority-and-resources-to-biometrics/*.

[3] *https://www.trade.gov/ttab/docs/TTAB__Biometrics%20Recommendations%20Letter__042-919.pdf*.

[4] The following statutes require DHS to take action to create an integrated entry-exit system: Section 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106–215, 114 Stat. 337; Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104–208, 110 Stat. 3009–546; Section 205 of the Visa Waiver Permanent Program Act of 2000, Pub. L. No. 106–396, 114 Stat. 1637, 1641; Section 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107–56, 115 Stat. 272, 353; Section 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), Pub. L. No. 107–173, 116 Stat. 543, 552; Section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. No. 108–458, 118 Stat. 3638, 3817; Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110–53, 121 Stat. 266, 338; and Section 802 of the Trade Facilitation and Trade Enforcement Act of 2015, Pub. L. No. 114–125, 130 Stat. 122, 199.

[5] [sic]

nies developed separate uses for biometrics, creating different guidelines and business rules, which increased privacy risks and decreased accountability, as each stakeholder had distinct responsibilities.

In 2017, CBP developed an integrated approach to the biometric entry-exit system that stakeholders, including other U.S. Government agencies with security functions, such as TSA, and travel industry stakeholders, such as airlines, airports, and cruise lines, could incorporate into their respective mission space. We 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 both biographic and biometric data (which is key to supporting CBP's mission), fulfilling the Congressional mandate and using the system to support air travel, and improve efficiency and the efficacy of identity verification, as stated below.

CBP has been testing various options to leverage biometrics at entry and departure.[6] These technologies will make the process for verifying the identity of individuals for this system more efficient, accurate, and secure by using facial comparison technology. However, the use of this technology allows CBP to improve identity verification. Using data that travelers voluntarily provide, we are simply automating the manual identity verification process done today. Facial comparison allows CBP to better identify those who are traveling on falsified or fraudulent documents, which improves our ability to identify those who are seeking to evade screening in order to enter the United States, including those who present public safety or National security threats, and visitors who have overstayed their authorized period of admission. Moreover, 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.

CBP has continuously kept Congress abreast of our process through several Congressional reports, hearings, and briefings. 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.[7]

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 to CBP, the U.S. Government and the private sector were already developing independent biometric solutions.

For example, from January 2004 through May 2007, DHS used kiosks placed between the security checkpoint and airline gates that would collect a traveler's fingerprint biometrics. The traveler had the responsibility to find and use the devices, with varying degrees of support from the airports where the kiosks were deployed. In 2008, DHS issued a Notice of Proposed Rulemaking (NPRM) proposing to require that 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 of the comments opposed the adoption of the proposed rule due to issues of cost and feasibility. Among other things, commenters suggested that biometric collection should be a purely governmental function, that requiring air carriers to collect biometrics was not feasible and would unfairly burden air carriers and airports, and that the highly competitive air industry could not support a major new process of biometric collection on behalf of the Government. Additionally, as directed by Congress, from May through June 2009, DHS operated two biometric exit pilot programs testing the collection of biometric exit data, first by CBP at the departure gate using a mobile device, and second by TSA at the security checkpoint.

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 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 IT infrastructure.

---

[6] Available at: *https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service-0.*

[7] Pub. L. 114–113 129 Stat. 2242 (December 17, 2015); Pub. L. 115–123 132 Stat. 64 (February 9, 2018).

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

Leveraging CBP's current authorities, we are executing Congressional mandates to test technologies to create an integrated biometric entry/exit system using facial comparison technology.[8] This technology uses existing advance passenger information could be used along with photographs already provided by travelers to the Government for the purposes of international travel to create "galleries" of facial image templates to correspond with who is expected to be on an international flight 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.[9] Once the gallery is created based on the advance information, the biometric comparison service compares a template of a live photograph of the traveler to the gallery of facial image templates. Live photographs are taken where there is clear expectation that a person will need to provide documentary evidence of their identity. If there is a facial image match, the traveler's identity has been verified.

These technologies will make the process for verifying the identity of individuals for this system more efficient, accurate, and secure by using facial recognition technology. For technical demonstrations at the land border, air entry, and some air exit operations, CBP takes photographs of travelers on CBP-owned cameras. These tests have been extended on a voluntary basis to exempt aliens[10] and U.S. Citizens. Such participation provides facilitative benefits and a more accurate and efficient method for verifying the identity and citizenship of these individuals. In other air exit and seaport demonstrations, CBP does not take the photographs; but specified partners, such as commercial air carriers, airport authorities, and cruise lines, take photographs of travelers and share the images with CBP's facial recognition technology. These partners that deploy their own camera operators and camera technology must meet CBP's technical and security requirements. These tests occur on a voluntary basis, and are conducted consistent with that partner's contractual relationship with the traveler.

CBP is authorized to require "in-scope"[11] aliens to provide biometric identifiers.[12] For entry, CBP is using facial comparison technology with CBP cameras during the inspection process.[13] For exit, CBP is operating pilot programs at certain land and sea ports of entry, and airports using facial comparison technology.[14] This technology provides the travel industry with the tools to use facial comparison to verify traveler identity and transmit information to CBP.[15] We have identified best practices from the prior work done by DHS as well as from our international partners that have informed the design of a biometric exit system that does not require an inefficient two-step process or require multiple different biometrics for traveler identity verification purposes.

---

[8] Available at: *https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service-0*.

[9] U.S. passport and visa photos are available via the Department of State's Consular Consolidated System. See Privacy Impact Assessment: Consular Consolidated Database, available at *https://2001-2009.State.gov/documents/organization/93772.pdf*.

[10] Under 8 CFR 235.1(f)(ii) and 8 CFR 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 any requirement to provide biometrics, including: Canadian citizens under section 101(a)(15)(B) of the Act 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 data 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 who hold E–1 visas 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 it 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.

[11] "In scope" aliens are aliens may be required to provide biometric identifiers to confirm their inadmissibility, or, at specified airports, their departure, under 8 CFR 235.1(f)(ii) and 8 CFR 215.8(a)(1).

[12] See 8 CFR 215.8(f)(ii), 235.8(a)(1).

[13] Available at: *https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service-0*.

[14] See 8 C.F.R. 215.8(a)(1).

[15] Numerous statutes require the advance electronic transmission of passenger and crew member manifests for commercial aircraft and commercial vessels. These mandates include, but are not limited to Section 115 of the Aviation and Transportation Security Act (ATSA), Public Law 107–71, 115 Stat. 597; 49 U.S.C. 44909 (applicable to passenger and crew manifests for flights arriving in the United States); Section 402 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSVERA), Public Law 107–173, 116 Stat. 543; 8 CFR 217.7; 8 CFR 231.1; 8 CFR 251.5; and 8 U.S.C. 1221.

CBP understood the need to build a system that all stakeholders within the travel continuum could participate in—without building their own independent system—that could expand to other mission areas outside of the biometric exit process. To address these challenges and satisfy the Congressional mandate, we work closely with our partners to integrate biometrics with existing identity verification requirements already required, to the extent feasible.[16]

The facial comparison technology utilized by CBP is currently able to match travelers at a rate of greater than 97 percent,[17] which is accomplished by comparing against a limited number of faces through the creation of galleries. Travelers who do not match to the system simply show their passport documents to a CBP officer or airline gate agent, and upon confirmation of identity, board the aircraft.

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 also to simultaneously improve the traveler experience throughout the travel continuum. CBP engineered a biometric exit solution that gives CBP, TSA, and industry stakeholders, such as airlines and airports, the ability to automate manual identity verification with facial comparison technology at locations where identity verification is present today. This may include the departure gates, debarkation areas, airport security checkpoints, and Federal Inspection Services (FIS) area. CBP only uses 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.

CBP AUTHORITIES AND REGULATORY UPDATES

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 of aliens to verify their identity, and authenticates travel documents presented by such aliens. Most recently, in 2017, Executive Order 13780 called for the expedited completion of the biometric entry-exit data system.[18]

DHS also has broad authority to control alien travel and to inspect aliens under various provisions of the Immigration and Nationality Act of 1952, as amended (INA).[19] As part of CBP's broad authority to enforce U.S. immigration laws, CBP is responsible for ensuring the interdiction of persons illegally entering or exiting the United States, facilitating and expediting the flow of legitimate travelers, and detecting, responding to, and interdicting terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States at entry. CBP also has responsibility to facilitate and expe-

---

[16] Ibid.

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

[18] Numerous other statues require DHS to take action to create an integrated entry-exit system including: Section 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106–215, 114 Stat. 337; Section 205 of the Visa Waiver Permanent Program Act of 2000, Pub. L. No. 106–396, 114 Stat. 1637, 1641; and Section 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107–56, 115 Stat. 272, 353.

[9] 8 U.S.C. § 1365b mandates the creation of an integrated and comprehensive system. This statute further provides that the entry and exit data system shall include a requirement for the collection of biometric exit data for all categories of individuals who are required to provide biometric entry data. 8 U.S.C. 1365b(d). 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 persons 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 of Dec. 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.

dite the flow of legitimate travel and trade and detect individuals attempting to illegally enter or exit the United States.

To effectively carry out its responsibilities under the INA upon both arrival and departure from the United States, CBP must be able to conclusively determine whether a person is in fact 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, which is material or relevant to the enforcement or administration of the INA.[20] 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.[21] Manual review of passports has historically been used to carry out this responsibility, but facial comparison technology can do so with greater consistency and accuracy.

CBP is statutorily mandated to fully implement a biometric entry/exit system, and has clear statutory authority to undertake all appropriate actions in support of the use of biometrics. To further advance the legal framework described above, CBP is working to propose and implement regulatory amendments and will provide progress updates in the Unified Agenda, as appropriate.

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 under this process 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 the November 2018 Privacy Impact Assessment,[22] we have developed Business Requirements to document this commitment, to which the private-sector partners must agree as a condition of participation in the pilots. Unlike with the pilots in the early 2000's, CBP has established these common system-wide standards (business requirements), which support CBP's integrated approach to the use of biometrics.

Regarding the recent subcontractor data breach incident, CBP is very concerned that the unauthorized access of CBP data will undermine Congressional and public confidence in CBP at a time in which we are pursuing transformative and innovative initiatives to enhance lawful trade and travel. We are aggressively investigating the breach of the subcontractor's systems and potential exposure of traveler and license plate images. There are two events that are under investigation: (a) A malicious cyber attack that impacted the systems of a Federal subcontractor; and (b) the unauthorized access of CBP data by the same Federal subcontractor.

This incident did not impact any of the air entry/exit partnerships discussed earlier and is limited solely to certain pilot program data collected in the land border environment. Airlines are trusted partners of CBP, given the various statutory airline collection mandates[23] in place. Airlines have been reliably providing CBP with advance electronic transmission of passenger and crew member manifests, as well as authenticating and verifying the identity of all passengers and ensuring that the traveling passengers are correctly documented to enter the receiving country.

While the data breach investigation is on-going, preliminary evidence indicates several violations of CBP privacy and security policies and violation of specific contract clauses. CBP is taking several actions to ensure the security of CBP systems, to include: Deploying cyber-enhanced technology (e.g., audit tracking, logging, and enhanced encryption) to all vehicle lanes to further protect license plate image data; conducting threat assessments to proactively identify vulnerabilities; restricting re-

---

[20] 8 U.S.C. 1357(b).

[21] 8 CFR 235.1(b). It is usually unlawful for a U.S. citizen to depart or attempt to depart from the United States without a valid passport. See 8 U.S.C. 1185(b); 22 CFR 53.1.

[22] Available at: *https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service-0*.

[23] Numerous statutes require the advance electronic transmission of passenger and crew member manifests for commercial aircraft and commercial vessels. These mandates include, but are not limited to Section 115 of the Aviation and Transportation Security Act (ATSA), Public Law 107–71, 115 Stat. 597; 49 U.S.C. 44909 (applicable to passenger and crew manifests for flights arriving in the United States); Section 402 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSVERA), Public Law 107–173, 116 Stat. 543; 8 CFR 217.7; 8 CFR 231.1; 8 CFR 251.5; and 8 U.S.C. 1221.

movable media usage and rolling out enhanced insider threat capabilities; and, updating all contractual, policy, and security requirements. Additionally, CBP required that the prime contractor immediately terminate its subcontracting agreement and its work thereunder. As such, the subcontractor no longer has access to CBP data.

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 obligations very seriously and are dedicated to protecting the privacy of all travelers. CBP complies with all requirements under the Privacy Act of 1974[24] (Pub. L. 93–579), as well as all DHS and Government-wide policies. In accordance with DHS policy, CBP uses the Fair Information Practice Principles (FIPPs) to assess the privacy risks and ensure appropriate measures are taken to mitigate any risks from its collection of data through the use of biometrics. As CBP is bound by the above-mentioned privacy laws and policies, as well as data collection requirements, partnering stakeholders are also held to the same standards, which increases accountability with the use of biometrics.

CBP strives to be transparent and provide notice to individuals regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII). When airlines or airports are partnering with CBP on biometric air exit, the public is informed that the partner is collecting the biometric data in coordination with CBP. We provide notice to travelers at the designated ports of entry through both physical and either LED message boards or electronic signs, as well as verbal announcements in some cases, to inform the public that CBP will be taking photos for identity verification purposes and of their ability to opt-out of having their photo taken.

Upon request, CBP Officers provide individuals with a tear sheet with Frequently Asked Questions (FAQ), opt-out procedures, and additional information on the particular demonstration, including the legal authority and purpose for inspection, the routine uses, and the consequences for failing to provide information. Additionally, in the FIS, CBP posts signs informing individuals of possible searches, and the purpose for those searches, upon arrival or departure from the United States.

Any U.S. citizen or foreign national may notify the airline-boarding agent that they would like to opt out at the time of boarding. The airline would conduct manual identity verification using their travel document, and may notify CBP to collect biometrics, if applicable.

CBP provides general notification of its biometric exit efforts and its various pilot programs through Privacy Impact Assessments (PIAs) and Systems of Records Notices (SORNs),[25] published at *www.dhs.gov/privacy,* and through information, such as Frequently Asked Questions, readily available at *www.cbp.gov.* We published a comprehensive PIA called the "Traveler Verification Service" in November 2018, to explain all aspects of CBP's biometric usage through the program, to include policies and procedures for the collection, storage, analysis, use, dissemination, retention, and/or deletion of data.[26]

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 bias. 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 in-scope[27] 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, and are held for this time period only in case of an extended system outage or for disaster recovery and are then deleted. We reduced the retention of U.S. citizen photos to no more than 12 hours as a direct result of briefings and consultations with Chairman Thompson.

Additionally, as described above, private-sector partners must agree to specific CBP business requirements, many of which are outlined in the recent PIA. CBP is simplifying the information flow to the traveling public by developing one set of

---

[24] 5 U.S.C. 552a.

[25] The 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. Those SORNs can be found at *https://www.dhs.gov/system-records-notices-sorns.*

[26] Available at: *https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service-0.*

[27] Pursuant to 8 CFR 215 and 235.

business standards and privacy guidelines, thereby enabling more comprehension of and transparency and accountability in the biometric process.

While CBP's commitment to transparency has been demonstrated by the above efforts, CBP is committed to improving its public messaging and helping the public better understand the technology. CBP welcomes the committee's input.

CBP collaborates regularly with the DHS Privacy Office to ensure compliance with applicable privacy laws and policies, and to build in privacy protection best practices surrounding CBP's use of biometric technology. 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.[28] CBP has implemented or is actively working to implement all of the DPIAC recommendations.

CBP is fully committed to the fair, impartial, and respectful treatment of all members of the trade and traveling public. CBP has rigorous processes in place to review data and metrics associated with biometric entry and exit facial comparison performance to assess and guard against improper bias. Significant variance in match rates that can be attributed to demographic variables have not been detected. Additionally, CBP is partnering with the National Institute of Standards and Technology (NIST) to conduct a comprehensive analysis of facial comparison technologies in CBP's biometric entry-exit efforts, in order to improve data quality and integrity, and ultimately the accuracy of technology that informs agency decision making that affects people. NIST will provide guidance and data that allows CBP to set a threshold, given CBP's security and facilitation goals for large-scale face recognition of travelers at air, land, and sea POEs.

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

Biometric Entry-Exit in the Air Environment

CBP is also enhancing the arrivals process by using facial comparison technology. With more efficient and more secure clearance processes, airports, airlines, and travelers benefit from shorter connection times and standardized arrival procedures. Security is increased by adding facial comparison as an additional tool to reduce imposter threat while increasing the integrity of the immigration system. Since initiating this facial comparison technology in the air environment on a trial basis, CBP has already identified 6 imposters,[29] including 2 with genuine U.S. travel documents (passport or passport card), who were using another person's valid travel documents as a basis for seeking entry to the United States.

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 continues on how they can be incorporated into the comprehensive entry-exit system, 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 simultaneously 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 the limitations outlined above and DHS's desire to implement the use of biometrics without negatively affecting

[28] *https://www.dhs.gov/sites/default/files/publications/Report%202019-01__Use%20of%20-Facial%20Recognition%20Technology__02%2026%202019.pdf.*

[29] Number of imposters updated as of June 11, 2019.

cross-border commerce, CBP plans on taking 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, Arizona POEs. CBP plans to expand to additional locations along the Southern Border in 2019. By using the facial comparison technology in the land environment, CBP has identified 138 imposters, including 45 with genuine U.S. travel documents (passport or passport card), attempting to enter the United States.

Additionally, CBP tested "at speed" facial biometric capture camera technology on vehicle travelers.[30] From August 2018–February 28, 2019, CBP conducted a technical demonstration of facial comparison technology on persons inside vehicles moving less than 20 miles per hour entering and departing Anzalduas, Texas.

Later in 2018, CBP began testing facial comparison technology at the Peace Bridge in Buffalo, New York in conjunction with the Buffalo and Fort Erie Public Bridge Authority (PBA) to facilitate the development of a demonstration project to test the viability of taking images from moving commercial trucks and comparing them against gallery images. From fall 2018 to early June 2019, PBA took photographs of truck drivers and sent them to CBP to assist with calibrating the project. The development is currently on pause.

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 (arrival) points at seaports.[31] Facial biometric processing at seaports replaces the current manual comparison performed by the CBP officer using the travel document. 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 4 sea entry sites and 4 major cruise lines that are operating facial comparison cameras to confirm the identity of arriving passengers on closed-loop cruises (which originate and terminate in the same city). The sea entry sites are Bayonne, New Jersey; Port Everglades, Florida; Miami, Florida; and Port Canaveral, Florida. Each cruise line conducting facial debarkation operations reports that passenger satisfaction feedback to include the debarkation process is significantly more positive as compared to such feedback from vessels not using facial debarkation. Engagement continues with cruise lines and port authorities to expand the technology to other businesses and locations.

CONCLUSION

DHS, in collaboration with the travel industry, is aggressively moving forward in developing a comprehensive biometric exit system in the land, air, and sea environments that simply replaces a manual identity check with facial comparison technology. The traveler is well aware that their picture is being taken for facial comparison purposes and more detailed information regarding the program is readily available to the public. CBP's collaborative biometric efforts directly addresses the recommendations of the 9/11 Commission Report, which highlighted 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."[32]

Chairman THOMPSON. Thank you for your testimony.

I now recognize Mr. Gould for summarize his statement for 5 minutes.

STATEMENT OF AUSTIN GOULD, ASSISTANT ADMINISTRATOR FOR REQUIREMENTS AND CAPABILITIES ANALYSIS, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. GOULD. Good morning, Chairman Thompson, Ranking Member Rogers, and distinguished Members of the committee. Thank you for inviting me before you today to discuss the future of bio-

[30] Available at: *https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service-0*.
[31] Ibid.
[32] The 9/11 Commission Report at 385–386, available at *http://govinfo.library.unt.edu/911/report/911Report.pdf*.

metric identification at the Transportation Security Administration. I am Austin Gould, the assistant administrator for requirements and capabilities analysis at TSA. I would like to thank the committee for working with TSA as we continue to improve the security of transportation systems and, particularly, for your support of our officers in the field.

The Aviation and Transportation Security Act of 2001 established TSA and the requirement to screen all passengers who were boarding aircraft. This screening requirement includes passenger identity verification. The act specifically mentions TSA's authority to use biometrics for this purpose. Recognizing the need to positively identify passengers in an era when fraudulent means of identification are becoming increasing prevalent and sophisticated, TSA has consistently sought new processes and technologies to improve performance while protecting a passenger's privacy. Biometrics represent such technology.

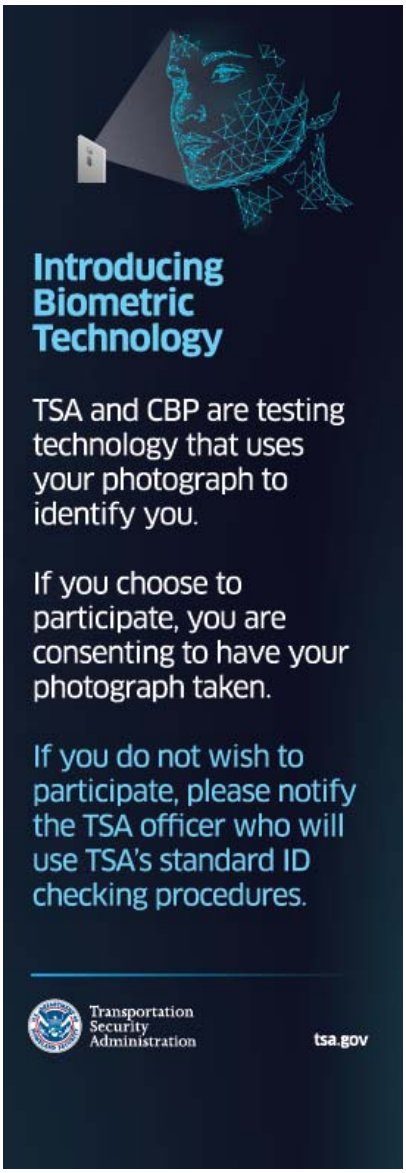
In 2018, TSA released a biometrics roadmap, which identifies the steps that the agency is taking to test and potentially expand biometric identification capability. The roadmap has 4 major goals: Partner with Customs and Border Protection on biometrics for international travelers; operationalize biometrics for TSA PreCheck passengers; potentially expand biometrics to additional domestic travelers; and develop the infrastructure to support these biometric efforts.

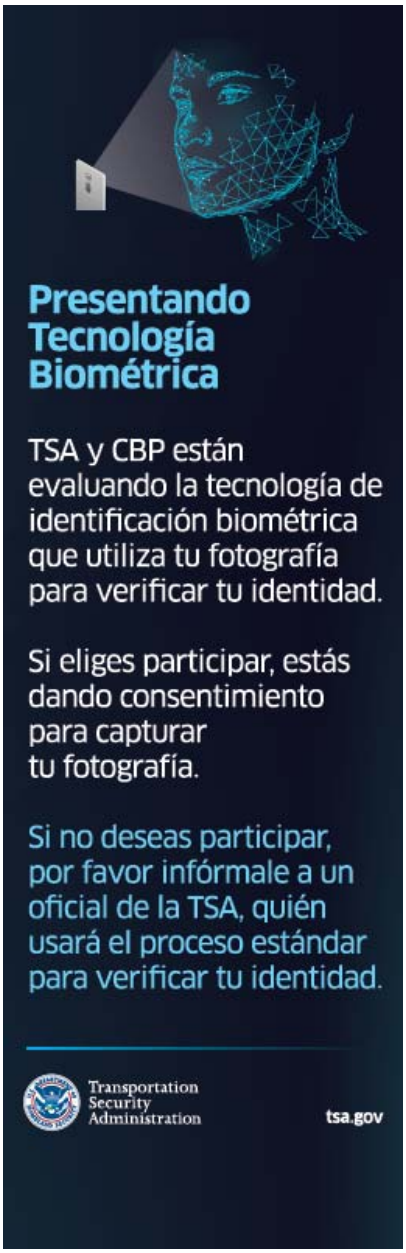
Consistent with the biometrics roadmap, TSA is conducting pilots that use facial biometrics to verify passenger identity at certain airports. These pilots are of limited scope and duration and are being used to evaluate biometric technology for TSA use. These pilots have been executed in conjunction with Customs and Border Protection, have been supported by privacy-impact assessments, and passengers have the opportunity to not participate. In these cases, the standard, manual identification process is used.

Last month, I observed the pilot currently under way in Terminal F in Atlanta for international passengers. The capture camera used for this pilot was in active mode, meaning that it only captured a facial image after the passenger was in position and the officer activated it. After the Committee on Government Oversight and Reform hearing on 4 June, TSA collected data in Atlanta that demonstrated that over 99 percent of travelers chose to use biometric identification.

Also, based on feedback from the hearing, we have deployed signage in both Spanish and English to ensure that passengers are aware that biometrics are being used and the procedure for opting out. An example of that signage is currently displayed on the monitor.

[The information follows:]


Introducing
Biometric
Technology
TSA and CBP are testing technology that uses your photograph to identify you.
If you choose to participate, you are consenting to have your photograph taken.
If you do not wish to participate, please notify the TSA officer who will use TSA's standard ID checking procedures.
Transportation Security Administration
tsa.gov



Mr. GOULD. TSA is committed to addressing accuracy, privacy, and cybersecurity concerns associated with biometric capture and matching. In that regard, and pursuant to section 1919 of the TSA Modernization Act, DHS will submit a report that includes assessments by TSA and CBP that were developed with the support of the DHS Science and Technology Directorate. The report will ad-

dress accuracy, error rates, and privacy issues associated with biometric identification.

We will also schedule a meeting with privacy groups later this summer to ensure that they understand TSA's limited use of biometric identification, have the opportunity to address any concerns, and as a follow-on to their participation in TSA's earlier Biometrics Industry Day.

Looking ahead, TSA plans to continue to build upon the success of past pilots by conducting additional ones at select locations for limited durations, to refine requirements for biometrics use. These pilots will continue to be supported by privacy-impact assessments, clearly identified through bilingual airport signage, and passengers will always have the opportunity to choose not to participate.

Biometrics represents a unique opportunity for TSA. This capability can increase security effectiveness for the entire aviation system, while also increasing throughput at the checkpoint and enhancing the passenger's experience. The ability to increase throughput while providing more accurate identification will be essential as passenger volumes continue to grow at approximately 4 percent annually. In fact, we experienced our busiest travel day ever last Sunday of the Fourth of July weekend when we screened approximately 2.8 million passengers and crew.

To close, TSA is systematically assessing biometrics for TSA use. This identification process will enhance aviation security while also increasing passenger throughput and making air travel more enjoyable. TSA's system will only be used for passenger identification and to direct the passenger to the appropriate level of screening, automating what is currently a manual process. It will not be used for any law enforcement purposes, and as always, passengers will have the opportunity to not participate.

Thank you for the opportunity to address this important issue before the committee, and I look forward to answering your questions.

[The prepared statement of Mr. Gould follows:]

PREPARED STATEMENT OF AUSTIN GOULD

JULY 10, 2019

Good morning Chairman Thompson, Ranking Member Rogers, and distinguished Members of the committee. Thank you for inviting me to testify about TSA's current work on assessing how biometric technology can potentially improve both the security and efficiency of our transportation system. In June 2018, I became the assistant administrator of TSA's Requirements and Capabilities Analysis (RCA) office. RCA is responsible for driving the strategy and development of TSA's security architecture and operational capabilities to enhance security and optimize mission performance through analysis and innovation. RCA directly supports TSA's mission by assessing current state operations, conducting gap analyses, managing needs identification, and developing requirements to generate new and improved security capabilities in alignment with the future vision of aviation security.

Assessing biometrics technology for application to TSA's missions is a key initiative for RCA. I welcome this opportunity to explain to the committee why TSA evaluates the potential to use facial recognition technology during its passenger screening process, how TSA leverages both the work and systems already developed by U.S. Customs and Border Protection (CBP), and the efforts we have taken to date, and continue to take, to ensure that cybersecurity, privacy, and civil liberties concerns are considered and addressed at every stage of biometric testing and potential deployment.

The U.S. aviation transportation system accommodates approximately 965 million domestic and international passengers annually—this equates to the screening of

roughly 2.2 million passengers, 1.4 million checked bags, and 5.1 million carry-on bags each day. In fiscal year 2018, TSA screened more than 804 million aviation passengers, representing a 5 percent volume increase from fiscal year 2017. Despite the significant progress the U.S. Government has made to improve transportation security, aviation hubs remain high-value targets for terrorists. Terrorist modes and methods of attack are more decentralized and opportunistic than ever before.

To stay ahead of these adversaries, we have to innovate, deploy new solutions rapidly and effectively, and make the most of our resources. In enacting the Aviation and Transportation Security Act in 2001, Congress recognized the importance of having TSA explore the use of biometric or similar technologies to enhance security in the aviation domain. As part of its mission to protect the Nation's transportation systems to ensure freedom of movement for people and commerce, TSA is exercising this authority to assess the use of biometrics technology, such as facial recognition, for identity verification, including at the checkpoint. Our evaluation of the use of biometrics technology is for the purpose of ascertaining how biometric technology might be used to automate passenger identity verification processes to fulfill a number of TSA security requirements, and relatedly, to determine a passenger's ability to access areas of the airport beyond the checkpoint.

Today, TSA Transportation Security Officers at the Travel Document Checker position at each checkpoint and airline employees at the check in desk visually compare the passenger in front of them to their photo ID to verify identity. TSA seeks to assess whether biometrics technology can automate these processes in ways that enhance security effectiveness, improve operational efficiency, and streamline the passenger experience. TSA's investment in Credential Authentication Technology (CAT) units provides a key tool through which the agency is analyzing how biometric facial recognition may be applied and optimized at the checkpoint. CAT authenticates the security features of a passenger's identification document and then displays the passenger's screening status from Secure Flight to ensures that the passenger has the appropriate flight reservation to progress through security screening and enter the sterile area. Currently, TSA is assessing the benefits of adding a front end camera to CAT units to further improve the identity verification process.

TSA recognized the need to outline a comprehensive approach for how it might develop and implement biometric solutions. To that end, TSA issued the *TSA Biometrics Roadmap for Aviation Security & the Passenger Experience,* which is available to the public on TSA's website, in September 2018. The *Biometrics Roadmap* centers on four goals:

- Partnering with CBP on biometrics for international travelers;
- Operationalizing biometrics for TSA PreCheck® travelers;
- Expanding biometrics to additional domestic travelers; and
- Developing support infrastructure for biometric solutions.

Equally important, the *Biometrics Roadmap* also established as a guiding principle that TSA will adopt a "privacy by design" mindset that incorporates privacy and civil liberty considerations into each phase of biometric solution development (design, build, implement). It also delineates that privacy protections will include restrictions to prevent the use of biometrics for purposes other than transportation security unless individuals have opted into other uses. Importantly, passengers will always have an option to not be processed through biometrics solutions at our checkpoint.

In 2004 Congress directed CBP to develop a biometric entry/exit program, and CBP has been developing and deploying an automated facial recognition solution since 2013 in order to comply with this mandate. Recognizing the opportunity to align and leverage similar operational efforts amongst DHS components, TSA signed an agreement with CBP in April 2018 on the development and implementation of joint work related to biometric technology at airports. Because of this partnership, TSA and CBP have collaborated on a series of multi-phased pilots using CBP's facial recognition technology, the Traveler Verification Service (TVS), for identity verification at the TSA checkpoint at three major airports.

- The first phase pilot, which TSA conducted at John F. Kennedy International Airport between October and November 2017, tested TVS's ability to perform facial matching for volunteer international outbound passengers at the TSA checkpoint. TSA did not alter any operational procedures during this phase.
- There were 2 second-phase pilot programs, also involving volunteer passengers. One occurred at Los Angeles International Airport from August to October 2018, and evaluated using TVS's facial matching results for passenger identity verification. The other pilot program, which began in November 2018 at Hartsfield-Jackson Atlanta International Airport in coordination with Delta Air Lines, is on-going and testing the long-term viability of biometrics at check-in, bag drop, and the checkpoint.

- The third phase of pilot programs will focus on TSA's ability to combine Secure Flight vetting status with the identification results from TVS's facial matching technology.

This deliberate, iterative approach to assessing facial recognition technology applications in TSA operations provides the agency with a significant learning opportunity as well as helping to refine future testing and pilot designs. We are grounding our exploration of biometric solutions in rigorous scientific study and analysis as well as ensuring appropriate privacy and cybersecurity safeguards are in place. While TSA and CBP coordinate efforts on passenger-facing biometrics today, TSA is also laying the groundwork for an eventual transition of relevant storage and matching capabilities to DHS Office of Biometric Identity Management (OBIM), an entity established by Congress to provide the Department with enterprise biometric solutions. TSA has engaged OBIM regularly on the build out of its next generation Homeland Advanced Recognition Technology, which will modernize and replace the legacy Automated Biometric Identification System, as well as to receive the benefit of their subject-matter expertise.

Based on the work of DHS S&T, the National Institute for Standards and Technology, and other researchers, we are aware of a variety of concerns related to differences in performance for travelers of different demographic groups and take this issue seriously. Some of these concerns pertain to risk of different error rates that correlate with user race, gender, and age. As required by the TSA Modernization Act (Public Law 115–254, Oct. 5, 2018), TSA studied matching performance differences across biometric systems and operational environments to identify the existence of disparities on these and other grounds. In fact, pursuant to this Act, TSA will provide a report to Congress that includes an assessment of these issues.

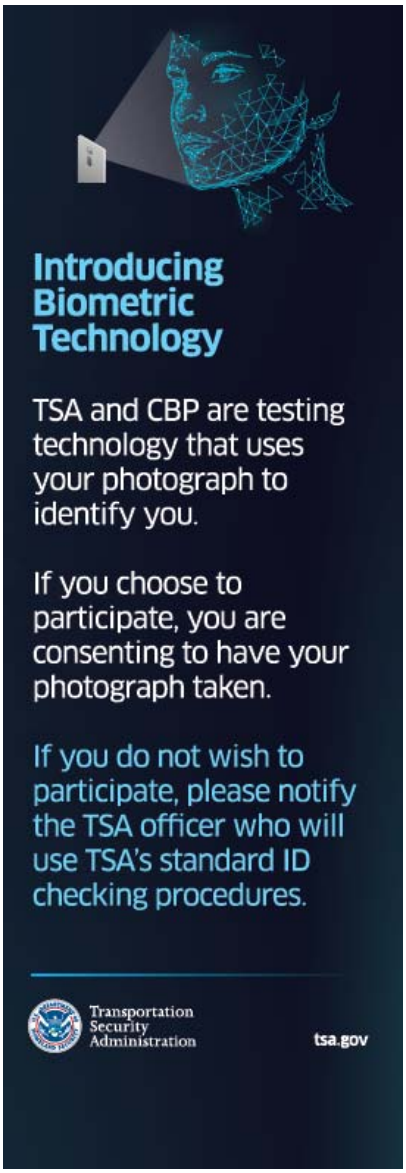
TSA also recognizes that biometric technologies pose unique privacy concerns. Reflective of such, TSA continually assesses privacy impacts and implements, as necessary, various strategies to address them in the passenger context. Should TSA fully operationalize this technology, it will mitigate privacy risks through providing robust notice and meaningful choice of alternatives, ensuring strong data security measures, deleting biometric data promptly following the passenger transaction, and focusing the uses of the biometric data to those directly necessary for transportation security, or as authorized under the Privacy Act of 1974, 5 U.S.C. § 552a. A number of publicly-available Privacy Impact Assessments (PIAs) on the Traveler Verification Service (TVS) and CBP's cloud-based facial matching system have been issued, which TSA has relied upon throughout the collaboration. These PIAs will be updated and strengthened as necessary as biometric identification develops further. They can be found on the DHS Privacy Office's public-facing website for review.

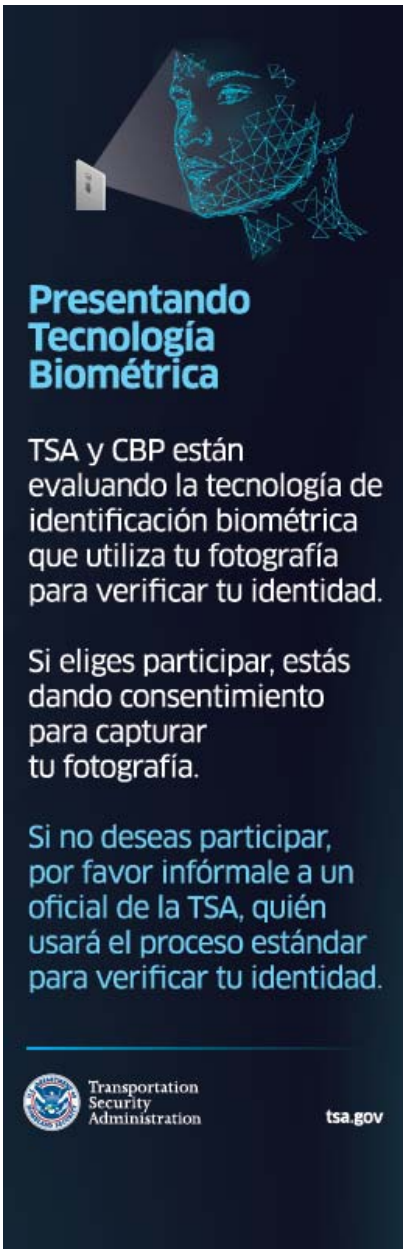
With regard to future endeavors, TSA is committed to protecting personally identifiable information, being transparent, and proactively mitigating privacy and civil liberties risks identified in the use of biometric technology. To that end, the DHS's Fair Information Practice Principles, known as the FIPPs, which serve as DHS's overarching privacy principles as applied across the Department, will guide efforts to protect privacy while achieving the operational and security benefits of biometrics technology.

Although TSA is still early in its exploration of biometric technologies, we are excited about the potential security benefits building this capability may provide. We plan to continue testing and evaluating biometrics technology in an operational context through additional pilot programs. TSA is planning for a pilot in the fourth quarter of this fiscal year at McCarran International Airport to test the 1:1 matching capabilities of the upgraded front-end CAT machine with a camera unit for facial recognition procedures in TSA PreCheck® lanes. This pilot will not involve CBP technologies or processes. TSA is finalizing the PIA for this pilot to ensure the public is aware of any pilot biometric technology solutions involving the collection, maintenance, use, or dissemination of personally identifiable information.

As reflected by TSA's March 2019 Biometrics Industry Day—an event attended by more than 120 people representing various public and private stakeholder groups including 5 different privacy advocacy organizations—we will continue to strive to foster communication, transparency, and input regarding our findings and approach to developing biometric solutions. Through the information we obtain from pilots and stakeholders, we hope to gain a better understanding of the operational impacts of this technology on travelers and consider that in developing procedures for the potential use of this technology at the checkpoint. TSA will continue to work on building a robust requirements and architecture foundation, develop an acquisition strategy, and seek to fulfill the goals identified in the Biometrics Roadmap.

Chairman Thompson, Ranking Member Rogers, and Members of the committee, thank you for the opportunity to testify before you today. I look forward to your questions.


Introducing
Biometric
Technology
TSA and CBP are testing technology that uses your photograph to identify you.
If you choose to participate, you are consenting to have your photograph taken.
If you do not wish to participate, please notify the TSA officer who will use TSA's standard ID checking procedures.
Transportation Security Administration
tsa.gov



Chairman THOMPSON. Thank you for your testimony.

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

STATEMENT OF JOSEPH R. DI PIETRO, CHIEF TECHNOLOGY OFFICER, U.S. SECRET SERVICE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. DI PIETRO. Good morning, Chairman Thompson, Ranking Member Rogers, and distinguished Members of the committee. I am Joseph Di Pietro, chief technology officer of the United States Secret Service. I want to thank you for the opportunity to appear before you today and to discuss the Secret Service's use of biometrics in performance of our integrated mission.

As previously conveyed to your committee staff, the Secret Service has significant concerns about testifying in an open hearing on how we use facial recognition technology to enhance our protective mission. Therefore, my testimony today on that issue will focus on the current facial recognition technology pilot program we are conducting at the White House complex. The Secret Service closely guards our means and methods as to how we execute our protective mission. We are aware that our adversaries are constantly watching and probing us and could potentially exploit information discussed in this open environment to use against us.

It would not be wise or prudent to discuss in a public setting certain assets, capabilities, and protocols used to carry out our protective mission. However, we would welcome the opportunity to provide this information to you in a closed briefing.

Biometric tools, such as fingerprint analysis and DNA collection, are used on a regular basis by the Secret Service to investigate, locate, and sometimes arrest individuals who have committed crimes, to include offenses related to threats against Secret Service protectees. We understand that the rapid expansion of biometric technology creates a need to balance capabilities with the need to preserve the public's expectation of privacy, and the Secret Service is committed to ensuring a balance that protects the rights of all individuals.

With respect to fingerprints and palm prints, the Secret Service has a long-standing program that plays an integral part in our investigative and personal security processes. Our ability to process, store, search, and retrieve fingerprint and palm print images is an operational necessity.

During the course of investigations involving fingerprint and palm print evidence, forensics examiners at the Secret Service utilize a variety of regional and National databases to search latent prints for matches to known subjects. With respect to DNA, DNA evidence is one of the most effective identification tools available to law enforcement today. Advancements related to DNA technology have been rapid, and the Secret Service remains dedicated to utilizing new applications to enhance our integrated mission.

The Secret Service collects DNA samples, along with a subject's fingerprints, as part of the identification and arrest process. Samples are sent to the FBI and DNA testing, search, and storage in the National DNA database.

With respect to facial recognition technology, the Secret Service recognizes that this technology has the potential to be a powerful tool that may assist in preventing attacks on our protectees, and there must be an appropriate balance between security and any potential privacy or other Constitutional concerns.

In 2014, former Secretary of Homeland Security Johnson established an independent protective mission panel to conduct an assessment of security at the White House complex. Among other important recommendations, the panel stated technology systems used on the complex must always remain on the cutting edge, and the Secret Service must invest in technology, including becoming a driver of research and development that may assist in its mission.

In furtherance of these recommendations, the Secret Service is currently working on a facial recognition pilot. The goal of the pilot is to determine whether facial recognition technology could be effectively deployed to enhance our protective mission. While the pilot started in December 2018 and is scheduled to be completed by the end of August 2019, the Secret Service began contemplating this pilot as far back as August 2014.

The participants in the pilot are Secret Service employees who volunteered to take part in this effort. Designated White House cameras that are part of the video management system captured the volunteers as they moved through various locations around the White House complex. Software running on a server dedicated to the pilot and on a closed network not connected to the internet seeks to match the images of the volunteers to the images in the video streams.

Facial images are stored when associated with a match to one of the volunteers, and at the conclusion of the pilot, all images will be purged.

The Secret Service's commitment to maintaining First Amendment protections and desire to address personal privacy consideration are central factors behind any future implementation of facial recognition technology. The Secret Service will not adopt new technologies unless they have been thoroughly vetted to ensure that sufficient privacy protections and data safeguards are in place.

In closing, the protection of our Nation's leaders is paramount to this agency and to the Nation. The partnerships represented here today, both in Congress and within DHS, are critical to the success of Secret Service operations.

I thank you for the opportunity to testify concerning the agency's use of these evolving technologies, and I look forward to working with you as we move forward. This concludes my testimony. I welcome any questions you have at this time.

[The prepared statement of Mr. Di Pietro follows:]

PREPARED STATEMENT OF JOSEPH DI PIETRO

JULY 10, 2019

Good morning Chairman Thompson, Ranking Member Rogers, and distinguished Members of the committee. I am Joseph Di Pietro, chief technology officer of the United States Secret Service (Secret Service). I want to thank you for the opportunity to appear before you today to discuss the Secret Service's use of biometrics in performance of our integrated mission.

As previously conveyed to your committee staff, we have serious concerns about testifying in an open hearing on how we use facial recognition technology to enhance our protective mission. Therefore, my testimony today on that issue will focus solely on the current pilot program we have in place at the White House Complex, as outlined in the Department of Homeland Security (DHS) Privacy Impact Assessment (PIA) dated November 26, 2018.

Pursuant to Title 18 U.S.C. § 3056, the Secret Service is authorized to protect the President, the Vice President, their immediate families, and other individuals enu-

merated in the statute. It is our responsibility to constantly research and evaluate the benefits and risks of applying available, new and emerging technologies to keep our protectees safe and to enhance the capabilities of our front-line Uniformed Division Officers, special agents, and mission support employees.

The Secret Service closely guards our "means and methods" as to how we execute our protective mission. It would not be wise or prudent to discuss in a public setting certain assets, capabilities, and protocols used to carry out our protective mission. We are aware that our adversaries are constantly probing us and could potentially exploit information discussed in this open environment to attack us.

The Secret Service uses biometric tools such as fingerprint analysis and DNA collection on a regular basis, in accordance with standards and policies, in order to investigate, locate, and sometimes arrest individuals who have committed crimes, to include offenses related to threats against Secret Service protectees.

Facial recognition technology is an effective tool that has the potential to act as a force multiplier. Accordingly, the Secret Service seeks to utilize and harness these important advances to enhance our effectiveness while upholding rights guaranteed by our Constitution.

FINGERPRINT/PALM PRINTS

The Secret Service has a long-standing fingerprint and palm print program that plays an integral part in our investigative and personnel security processes. The Secret Service's ability to process, store, search, and retrieve fingerprint and palm print images is an operational necessity.

The Secret Service Live-Scan Program (SSLSP) is an enterprise-wide initiative deploying Live-Scan Booking Stations to Secret Service offices agency-wide. Live-Scan Booking Stations electronically capture, digitize, and transmit descriptive information, fingerprints, palm prints, signatures, and photos of both applicants and investigative subjects who are processed through these stations. The records are transmitted to the Federal Bureau of Investigation's (FBI) Next Generation Identification System (NGI) database for an automated search against over 76 million criminal fingerprint records. Simultaneously, these records are submitted to the Secret Service's own database for searching and archiving. The conduit used to forward the information to the FBI is the U.S. Department of Justice's Joint Automated Booking System (JABS).

During the course of investigations involving fingerprint and palm print evidence, forensic examiners at the Secret Service utilize a variety of regional and National databases to search latent prints for matches to known subjects. For example, the Secret Service coordinates directly with the FBI and the DHS via their databases, to include the DHS Office of Biometric Identity Management's Automated Biometric Identification System (IDENT).

DNA

DNA evidence is one of the most effective identification tools available to law enforcement today. Advances related to DNA technology have been rapid, and the Secret Service remains dedicated to utilizing new applications to enhance our integrated mission. DNA technology can provide accurate identification, improve prosecution rates, and act as a deterrent against future criminal acts.

The Secret Service collects DNA samples along with a subject's fingerprints as part of the identification and arrest process. Buccal collection kits from the FBI are used during the booking process and are then returned to the FBI for DNA testing, search, and storage in the National DNA database.

FACIAL RECOGNITION TECHNOLOGY

In 2014 former Secretary of Homeland Security Johnson established an independent Protective Mission Panel (PMP) to conduct an assessment of the security at the White House complex. Among other important recommendations, the PMP stated that, "[t]echnology systems used on the complex must always remain on the cutting-edge, and the Secret Service must invest in technology, including becoming a driver of research and development that may assist in its mission."[1]

Facial recognition technology is a significant tool currently being used with great effectiveness in both the private and Government sectors. Accordingly, the Secret Service is evaluating the potential benefits of this technology to this agency's protective mission. Applied correctly and with appropriate controls, this technology could

[1] See *Executive Summary to Report from the United States Secret Service Protective Mission Panel to the Secretary of Homeland Security,* 2014, p. 7.

potentially be used by the Secret Service to enhance our security posture at critical protective venues.

Specifically, this technology may have the potential to provide an early notification to Secret Service personnel of individuals who are of record with the agency when they approach a protective site. These individuals would have already made a threat against one of our protectees or been shown to have expressed an "unusual interest" toward one of our protectees and, therefore, pose a serious threat to protected persons, venues, or the general public in close proximity to one of our protected sites.

While the benefits of technology associated with facial recognition may provide greater capabilities than the observations of law enforcement personnel, the Secret Service is well aware that there must be an appropriate balance between security and any potential privacy or other Constitutional concerns. Further, it is noted that the Secret Service expects to come in contact with thousands of the general public around the White House every day and that the men and women of the agency strive to ensure a secure environment while respecting all individual's Constitutional rights.

FACIAL RECOGNITION PILOT (FRP)

In furtherance of the 2014 PMP report recommendations, the Secret Service Office of Technical Development and Mission Support is currently working on a Facial Recognition Pilot (FRP). The goal of the FRP is to determine whether facial recognition technology could be effectively deployed to enhance the Secret Service's protective mission. In addition, the Service will determine whether this technology would be a fiscally responsible investment that would assist in identifying subjects of interest to the Secret Service as they approach a protected site.

While the FRP started in December 2018 and is scheduled to be completed by the end of August 2019, the Secret Service began contemplating this pilot in August 2014. Prior to the initiation of the program, DHS approved and published a Privacy Impact Assessment, evaluating the privacy risks and associated mitigation strategies.[2]

The participants in the FRP are Secret Service employees who volunteered to take part. These individuals had their images loaded into the FRP server. Video streams capture the volunteers as they move through various locations around the White House Complex, and images of the volunteers are matched to the video streams. Subsequently, volunteers provide notification of their movements in and around the Complex for comparison with the generated matches in the system.

The video streams feed into both the White House CCTV system and into the FRP server. The FRP server is operated on a closed network and is not capable of remote connections. The data collected is stored in a stand-alone database dedicated only to the pilot testing. Only individuals cleared by the Secret Service have access to the collection database, and they are accompanied by agency personnel while accessing the FRP server. All Secret Service personnel and supporting contractors with access to the data undergo annual privacy awareness and document security training. Facial images are stored when associated with a match to one of the volunteers, and, at the conclusion of the FRP, all images will be purged.

The data collected throughout the FRP will be evaluated for its effectiveness and accuracy.

OFFICE OF BIOMETRIC IDENTITY MANAGEMENT (OBIM)

The Secret Service recognizes the value offered by OBIM and its biometric data storing, matching, and sharing capabilities to assist with both our protective and investigative functions. Developing a partnership with OBIM will provide a valuable means to search, match, and store our biometric data across DHS components as well as with external agencies. The Secret Service maintains coordination with OBIM liaisons and continues to develop capabilities and policies regarding the use, storage, and dissemination of biometric information.

CONCLUSION

The protection of our Nation's leaders is paramount to this agency and to the Nation. The partnerships represented here today, both in Congress and among those of us within DHS, are critical to the success of Secret Service operations. I thank you for the opportunity to testify concerning the agency's use of these evolving technologies, and I look forward to working with you as we move forward.

---

[2] DHS/USSS/PIA–024 Facial Recognition Pilot (Nov. 26, 2018).

Chairman Thompson, Ranking Member Rogers, and distinguished Members of the committee, this concludes my testimony. I welcome any questions you have at this time.

Chairman THOMPSON. Thank you for your testimony.

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

STATEMENT OF CHARLES H. ROMINE, PH.D., DIRECTOR OF INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE

Mr. ROMINE. Chairman Thompson, Ranking Member Rogers, and Members of the committee, I am Chuck Romine, director of the Information Technology Laboratory at the Department of Commerce's National Institute of Standards and Technology, or NIST. Thank you for the opportunity to appear before you today to discuss NIST's role in biometric standards and testing for facial recognition technology.

In the area of biometrics, NIST has been working with public and private sectors since the 1960's. 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 on biometrics recognition. 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 communications systems that are interoperable, reliable, secure, and useable.

NIST's biometric evaluations advance the technology by identifying and reporting gaps and limitations of current biometric recognition technologies. NIST's 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.

Since 2000, NIST's Face Recognition Vendor Testing Program, or FRVT, has assessed capabilities of facial recognition algorithms for one-to-many identification and one-to-one verification.

NIST expanded its facial recognition evaluations in 2017. NIST broadened the scope of its work in this area to understand the upper limits of human capabilities to recognize faces and how these capabilities fit into facial recognition applications.

Historically and currently, NIST's biometrics research has assisted the Department of Homeland Security, DHS. NIST's research was used by DHS in its transition from 2 to 10 prints for the former US–VISIT Program. Currently, NIST is collaborating with DHS OBIM on face image quality standards and with DHS Customs and Border Patrol on the evaluation of their traveler verification service.

NIST is working with DHS Customs and Border Patrol to analyze performance impact due to image quality and traveler demographics, and provide guidance and data that allows CBP to set a threshold, given CBP's security and facilitation goals for large-scale face recognition of travelers.

NIST's Face Recognition Vendor Testing Program was established in 2000 to provide independent evaluations of both prototype and commercially-available facial recognition algorithms. Significant progress has been made in algorithm improvements since the program was created.

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 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.

Optimal face identification was achieved only when humans and machines collaborated. As with all areas for face recognition, rigorous testing and 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.

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

[The prepared statement of Mr. Romine follows:]

PREPARED STATEMENT OF CHARLES H. ROMINE

JULY 10, 2019

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). NIST 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 biometrics 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 the 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 a 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 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.

Facial recognition technology compares an individual's facial features to available images for identification or authentication. Facial detection technology determines whether the image contains a face. Facial analysis technology aims to identify attributes such as gender, age, or emotion from detected faces.

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;
- 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 Federal agencies that depend upon biometrics recognition.

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; more than 100 biometric experts from all around the globe traditionally attend. 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 image characteristics such as noise or compression, and to subject characteristics such as age or gender. NIST biometric evaluations advance the technology by identifying and re-

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

porting 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 biometrics evaluations are highly regarded and valued by developers, users, and policy makers.

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.

To better align NIST's evaluation schedule with the pace of facial recognition advancement in industry and academia, NIST expanded its facial recognition evaluations in 2017. NIST broadened the scope of its work in this area to understand the upper limits of human capabilities to recognize faces and how these capabilities fit into facial recognition applications. NIST evaluations have quantified accuracy for investigative-use cases which involve human review of candidates from an automated system, as well as for fully automated identification applications in which decisions would be accepted on the basis of an automated search alone.

NIST's work on demographic effects in facial recognition is on-going. For example, a report addressing demographic effects in mugshots collected in domestic law enforcement applications is under development with an expected publication date of Fall 2019.

NIST provides technical guidance and scientific support for analysis and recommendations for utilization of facial recognition technologies to various Federal 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. Further, as DHS S&T works with Transportation Security Administration (TSA) to scientifically analyze data from its biometrics pilots to inform TSA's capability development process, NIST has and will continue to provide consultation to DHS S&T to assure its analysis methodologies meet industry standards.

Historically and currently, NIST biometrics research has assisted DHS. NIST's research was used by DHS in its transition from 2 to 10 prints for the former US–VISIT program and NIST is currently 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 program. Currently, NIST is collaborating with DHS CBP on the evaluation of their Traveler Verification Service (TVS), and with DHS OBIM on face image quality standards.

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 Federal 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 1 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,[2] showed that massive gains in accuracy have been achieved since the FRVT in 2013, which far exceed im-

[2] *https://www.nist.gov/publications/ongoing-face-recognition-vendor-test-frvt-part-2-identification.*

provements made in the prior period (2010–2013). The accuracy gains observed in the 2018 FRVT 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 one quarter of 1 percent of searches. These failures are mostly associated with images of persons with facial injury and those with a long time lapse (17 years or more for the most accurate algorithm) 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.

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,[3] 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,[4] 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 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 standards development organizations are appropriate or adaptable for the Government's purposes. OMB Circular A–119 directs the use of such standards by Federal 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 lines 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 standards development organization. Under accreditation by ANSI, the private-sector U.S. standards federation, NIST continues

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

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

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.[5] This standard continues to evolve to support Government applications including law enforcement and 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. Documents issued by large international organizations, such as the International Civil Aviation Organization 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 plays a leading role in 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 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. I would be happy to answer any questions that you may have.

Chairman THOMPSON. Thank you very much for your testimony. I now recognize myself for 5 minutes of questioning.

Mr. Wagner, you talked a little bit about the biometric, entry-and-exit system, and those of us who have been around, we have historically supported that system. But in the beginning, we talked about that system would be only used for foreigners, and based on what I heard you talk about today, you have expanded that to take in American citizens. Can you explain the reasoning for that?

Mr. WAGNER. Yes. U.S. citizens are clearly outside the scope of the biometric entry-exit tracking. The technology we are using for the entry-exit program we are also using to validate the identity of the U.S. citizen. Because someone has to do that. Someone has to determine who is in scope or out of scope, and someone has to validate that the U.S. citizen is the person presenting that U.S. passport.

So, once we take the picture and match it against the passport photo, which is what goes on right now just in a manual review, we use the algorithm to help make that decision, and then the photo is discarded after that because there is no need for us to save it.

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

Chairman THOMPSON. Well, and what I am trying to get at is, this was a policy that CBP more or less expanded even though Congress gave you the authority to look at foreigners.

Mr. WAGNER. Well, it helps us in the airlines determine who is in scope for biometric exit and who is out, because someone has to make that determination at the boarding area. It would be unfair to ask the airline to be able to do that, to determine who is in scope or out of scope.

Chairman THOMPSON. But you kind-of see what I am saying, though. Did CBP come back and say to Congress, we are looking at expanding this authority, but we need Congressional approval?

Mr. WAGNER. We don't see this as expanding the biometric entry-exit authority. We see this as using the authorities we have to determine the citizenship of an individual entering or departing the United States. If we are looking for a U.S. citizen departing the United States right now because they have a warrant for their arrest, we will stop travelers in the jet way and check their passports.

Chairman THOMPSON. I understand why you are doing it.

Mr. WAGNER [continuing]. Using authorities——

Chairman THOMPSON. Yes, I understand why you are doing it, but what I am getting at is part of this hearing is to make sure that we, as Members of Congress, give you the authority you need to do your job. But part of what I am hearing is you have kind-of taken your own initiative to do some things beyond the scope of authority that Congress gave you. So what I would like for you to do is provide the committee with the written policy by which you are doing this.

Mr. WAGNER. Yes, absolutely.

Chairman THOMPSON. Thank you. Dr. Romine—I am going to try to get it right—you have been advising DHS a lot on some of these things. Have you looked at this expansion of authority without Congressional intent with DHS?

Mr. ROMINE. No, sir. That would be outside of NIST's mission space, which is technical evaluation and standards of the algorithms.

Chairman THOMPSON. All right. Well, have you looked at the collection of data and how the data management is controlled once its collected?

Mr. ROMINE. No, sir.

Chairman THOMPSON. Mr. Wagner, I am back to you, then. Explain to the committee, this collection of data that you say this policy gives you, what do you do with it?

Mr. WAGNER. So, when the picture is taken and provided and comes into CBP and we match it against one of our pre-staged gallery photos, that is comprised of passports and visas and previous arrivals, if it is a foreign national, subject to the biometric entry-exit mandate, that photograph will be sent over to DHS, to OBIM, to be stored in IDENT, which is the Department's repository for that information. If it is a U.S. citizen and that photo matches a U.S. passport or a permanent resident or somebody outside of the scope of entry-exit, that photograph would be held for 12 hours and then deleted or purged from our systems. The only reason we hold

it for that short period of time is just in case the system crashes, and we have to restore everything.

Chairman THOMPSON. OK. Are you aware of the recent subcontractor breach of data?

Mr. WAGNER. Oh, yes.

Chairman THOMPSON. Beg your pardon.

Mr. WAGNER. Yes.

Chairman THOMPSON. So how is that inconsistent with what you just explained to us?

Mr. WAGNER. What we were doing with that subcontractor, is we were testing their camera on the U.S.-Mexico land border in a stand-alone pilot system. So it wasn't integrated into the main CBP network. We were testing the taking of the photographs and the license plates and the ability to take a picture of a person in a vehicle and whether that would be matchable. In this case, apparently the—as far as I understand, the contractor physically removed those photographs from the camera itself and put it onto their own network, which was then breached. The CBP network was not hacked. The contractor—and what we see is—what I believe is they removed that in violation of the contract, and that is why a relationship has been severed with them, and we are conducting an investigation.

Chairman THOMPSON. So you see my concern about how we control the data we collect?

Mr. WAGNER. Absolutely.

Chairman THOMPSON. Thank you.

I yield to the Ranking Member.

Mr. ROGERS. Thank you, Mr. Chairman.

Mr. Wagner, I want to pick up on what the Chairman is talking about. My understanding of your response a few moments ago is that it is your belief that you have the existing statutory authority to do what you are doing. You are just exercising new technology in that process. Is that an accurate representation of what your answer was?

Mr. WAGNER. Yes.

Mr. ROGERS. Thank you.

Dr. Romine, this has been an evolving technology. Can you tell us, what have been the big changes, if any, over the last 5 years, when it comes to the use of facial recognition, and biometrics in general?

Mr. ROMINE. Certainly. Thank you. The advances have been dramatic, according to our testing. The accuracy and capabilities of the newer systems that we have seen in the last few years——

Mr. ROGERS. What would be some examples of newer systems?

Mr. ROMINE. The advent of convolutional neural networks as machine learning capability to do the image analysis or image matching.

Mr. ROGERS. Is that AI, is that what you are talking about?

Mr. ROMINE. It is machine learning and artificial intelligence, yes, sir.

Mr. ROGERS. What else?

Mr. ROMINE. So these are dramatically improved over previous technologies that relied specifically on particular characteristics of faces, for example. With suitable training, these systems have dra-

matically improved the accuracy for the best facial recognition systems.

Now, I want to be clear, for the testing that we have done, there is still a very wide range of performance in the testing that we have done, in the algorithms that we have tested, but the best ones—and we have no direct knowledge of the convolutional neural networks or the machine learning, because these are submitted to us as black boxes and we don't examine that. But in conversations with vendors who have submitted testing, that is the understanding that we have, is that that new machine learning capability, that deep neural networks has been the significant advance.

Mr. ROGERS. Has this development or this advancement in the machine learning alleviated in any way the concerns the Chairman expressed about facial recognition being less accurate when it comes to females or darker-skinned individuals?

Mr. ROMINE. We see, because of the significant increases in the accuracy across the board, the effect of those demographic effects is diminishing. We have a report—we are doing an analysis now, a comprehensive analysis, of demographic effects under the testing that we have just done, and that report should be out this fall.

Mr. ROGERS. Great. When you have these test results, do you share those with not only DHS and the agency but the public, the business community?

Mr. ROMINE. We do, sir.

Mr. ROGERS. Great.

Mr. ROMINE. We do that through public reporting and also through dissemination with email and other interested parties.

Mr. ROGERS. Do you publish those guidelines for the public consumption as well?

Mr. ROMINE. We do. Yes, sir.

Mr. ROGERS. Excellent. Mr. Chairman, I have a letter here from the Security Industry Association supporting the use of biometrics and facial recognition, and I would like to offer it for the record.

Chairman THOMPSON. Without objection.

[The information follows:]

LETTER FROM DON ERIKSON TO CHAIRMAN BENNIE G. THOMPSON AND RANKING MEMBER MIKE D. ROGERS

July 10, 2019.

The Honorable BENNIE THOMPSON,
Chairman, House Committee on Homeland Security, 310 Cannon House Office Building, Washington, DC 20515.

The Honorable MIKE D. ROGERS,
Ranking Member, House Committee on Homeland Security, 310 Cannon House Office Building, Washington, DC 20515.

DEAR CHAIRMAN THOMPSON AND RANKING MEMBER ROGERS: On behalf of the Security Industry Association (SIA), thank you for holding a hearing on facial recognition technology. SIA represents over 1,000 companies that provide safety and security technology solutions vital to public safety, protecting lives, property, information and critical infrastructure.

The Security Industry Association (SIA) believes all technology products, including facial recognition, must only be used for purposes that are lawful, ethical and non-discriminatory. Advanced image and video analysis can and should be a catalyst for good. Facial recognition has proven to be a force multiplier for efforts to protect the homeland, assist law enforcement, and enhance the mission capabilities, efficiency, and effectiveness of operations in diverse ways. However, arbitrary limits will harm Americans who benefit from it in countless but underpublicized ways.

We are concerned that recent calls to completely ban the use of facial recognition technology at various levels of government are based largely on a misleading picture of how the technology works and its real-world uses in the United States. Such calls misunderstand the role of accuracy rates in everyday usage of facial recognition systems and misconstrue the real-world implications when algorithms may not work as well as intended.

Responsible use of facial recognition technology ensures that appropriate transparency and accountability measures, stakeholder education, and privacy considerations and civil liberties protections are equally taken into account prior to deployment. Further actions may be needed to reassure the public about how facial recognition technology is being used and ensure that proper policies are being followed. However, such actions must be based on sound analysis and involve input from stakeholders with expertise on the technology.

Prior to considering any legislation impacting the use of facial recognition technology, we strongly encourage Members to review SIA's recently published policy paper entitled, *Face Facts: Dispelling Common Myths Associated with Facial Recognition Technology* and the U.S. Department of Justice's Bureau of Justice Assistance *Policy Development Template,* which was published in concert with the U.S. Department of Homeland Security and other law enforcement stakeholders, for law enforcement use of the technology.*

SIA and our members stand ready to contribute to a constructive dialog surrounding facial recognition technology. Please let us know if there is any way we can assist you as you continue to examine these issues.

Sincerely,

DON ERICKSON,
CEO Security Industry Association

Mr. ROGERS. With that, I yield back. Thank you.

Chairman THOMPSON. Thank you.

Dr. Romine, just so we are clear, the report you referenced is not out.

Mr. ROMINE. That is correct, sir. It should be out this fall.

Chairman THOMPSON. So the data right now is that women and dark-skinned people are misidentified more than anybody else?

Mr. ROMINE. There are demographic effects that affect age—so significant changes in age over time—age, race, and sex, there are demographic effects. Quantifying those in a statistically valid manner is what we are currently doing.

Chairman THOMPSON. So is that women and dark-skinned people?

Mr. ROMINE. Yes.

Chairman THOMPSON. OK. Thank you. I am just trying to—thank you.

The Chair recognizes Mr. Correa for 5 minutes.

Mr. CORREA. Thank you, Mr. Chairman, for bringing up this most important issue. This technology is very interesting because compared to fingerprints, DNA, you give it without essentially giving permission. You walk down a corridor, some camera picks you up, picks up your information, and it is used without your authority or permission in ways that we don't know about.

Dr. Romine, you talked about false positives, based on ethnicity, other factors that are still—that technology has not gotten to the point where it can account for these factors.

Mr. Wagner, I have a question for you, which is, under the TSA Modernization Act of last year, it requires a public report on the deployment of biometric technologies, TSA's assessments of privacy

*The attachment has been retained in committee files and is available at *https://www.securityindustry.org/report/face-facts-dispelling-common-myths-associated-with-facial-recognition-technology/*.

accurate. That report is now late. Any thoughts of when that report can be presented to us?

Mr. WAGNER. Sure. The report is drafted. It is just circulating for final approval and signature.

Mr. CORREA. So at any time now?

Mr. WAGNER. Any time.

Mr. CORREA. OK. Will that be something that will be compared to Dr. Romine's report also that will be coming out very soon?

Mr. GOULD. Sir, moving forward, from a TSA perspective, we will look at any scientific reports and data that we possibly can to ensure that biometric identification is performing optimally for our use cases, yes, sir.

Mr. CORREA. So, before we get that report, let me, nonetheless, ask you, Mr. Wagner, right now, the way facial recognition is being used by your Department, is that affecting or unduly burdening foreign travelers, race, gender, nationality?

Mr. WAGNER. No. We are not seeing—in a review of our data, we are not seeing any significant error rates that are attributable to a specific demographic. That is why we have also partnered with NIST to come in and review our data and help us look at it and make sure.

Mr. CORREA. So statistically you do have Mr. Gould, is it, that is reviewing this data, or who is reviewing this data for you? To make sure that——

Mr. WAGNER. They are——

Mr. CORREA [continuing]. What you are saying your conclusion is that it is not adversely affecting commerce, tourism? I am from the State of California, where commerce, tourism, is a big part of our economy. I just want to make sure we are not having a lot of false negatives.

Mr. WAGNER. This is having a beneficial effect on that because it is allowing airlines and cruise lines to board and unboard people quicker.

Mr. CORREA. Excellent. Want to hear that. Just want to make sure that we see that in the report.

Mr. WAGNER. The passenger experience is being improved by that. We are reviewing internally our own data, and we are not seeing noticeable discrepancies in that. But we have partnered with NIST, and throughout this summer and fall, we will be examining our data very closely to make sure that we are not unduly hurting people of a specific demographic.

Mr. CORREA. I am glad to hear your enthusiastic, you know, positive answer that it is not burdening unduly some of those travelers.

Mr. WAGNER. Absolutely. We are not——

Mr. CORREA. Because that great Californian Ronald Reagan said: We got to trust, but we got to verify, too.

Mr. WAGNER. Absolutely.

Mr. CORREA. So I look forward to seeing your data on that and making sure we are on it. In terms of the data, the purging of the data, once you are using it, what system do you have to audit to make sure that that data is actually purged in a timely manner? You just mentioned one of your subcontractors had a breach. That information is somewhere out there. You said that is the reason you terminated that contract. Yet, to me, when that information

gets out there, terminating a contract is not enough of a—let's say, a deterrent to making sure that those kinds of breaches, that data, is actually purged in a timely manner. Are you doing anything to make sure that we tighten up that part of your system?

Mr. WAGNER. Yes. So the subcontractor may face subsequent action depending on the results of the——

Mr. CORREA. Criminal? Civil?

Mr. WAGNER. Potentially.

Mr. CORREA. Both?

Mr. WAGNER. Potentially. Depending on what the investigation—and our Office of Professional Responsibility is investigating this, I believe the IG is investigating this—depending on the circumstances of how the data was taken and the intentions and why, you know, how it was used, there potentially could be criminal actions or——

Mr. CORREA. When you have those data breaches, who do you report those to, and under what time do you actually take to say, "Hey, this purge—or this breach happened"?

Mr. WAGNER. Well, they are supposed to report it to us almost immediately. We do report it to Congress if it meets a certain threshold. Then internally we will——

Mr. CORREA. What threshold would that be?

Mr. WAGNER. I don't know off-hand.

Mr. CORREA. Like to look at that a little closer because clearly small breach versus a large breach, is that your threshold, size of the breach? What is the threshold?

Mr. WAGNER. I believe it is a hundred thousand, but I will have to—I will get back to you on that.

Mr. CORREA. Mr. Chairman, I am out of time, but I think it is very important that these kinds of breaches be reported immediately to Congress.

Chairman THOMPSON. I agree.

Mr. CORREA. Mr. Chairman, I am out of time, so I yield.

Chairman THOMPSON. Thank you very much. The Chair recognizes the gentleman from Texas, Mr. McCaul, for 5 minutes.

Mr. MCCAUL. Thank you, Mr. Chairman. You know, we all want to protect civil liberties and privacy. When somebody is in the public domain, as I understood in law school, there is no expectation of privacy. This technology, in my judgment, has really protected the Nation from drug smugglers, gang members, and potential terrorists.

I introduced the BITMAP bill, which is the Biometric Transnational Migration Alert Program. Last Congress, it passed unanimously out of this committee. It passed on the House floor, 272 to 119. Now it is being held up. I would like to examine what the effect of not authorizing this program would have.

Mr. Wagner, can you tell me what successes the BITMAP program has had? Particularly when it comes to individuals coming from other parts of the world, that are known—that are basically countries of special interest, special interest aliens, or KSTs, known or suspected terrorists, coming across, into this hemisphere up through Latin America, into the United States of America?

Mr. WAGNER. Sure. So the BITMAP Program, it is administered by ICE. It is a program they work with their foreign counterparts

to utilize fingerprint technology, to take fingerprints of exactly those populations you just referenced, as they transit through certain countries in Central or South America, making their way on up through Mexico to the United States. So, if they show up in a Central American country, the foreign authorities will use the BITMAP Program to collect the passport information and their fingerprints.

When that person ultimately shows up at our Southwest Border and has mysteriously lost their passport, we are able to take their fingerprints and match it back up with that previous encounter in Central America to sufficiently identify who that person is. This is the passport that they had at that——

Mr. MCCAUL. Is it true that, through that journey, that they are—while the names and identities may change——

Mr. WAGNER. Sure.

Mr. MCCAUL [continuing]. Their biometrics do not change?

Mr. WAGNER. Correct.

Mr. MCCAUL. That is the best way to identify who this person really is?

Mr. WAGNER. Correct.

Mr. MCCAUL. Can you, in this setting—and I don't know if that is possible—give us some indication of the numbers of special interest aliens that have been stopped in this program and also known or suspected terrorists?

Mr. WAGNER. Have to get back to you on that. I don't have any today.

Mr. MCCAUL. How significant is it?

Mr. WAGNER. It is significant. I mean, it is an absolute vulnerability that, as we have seen, terrorists can exploit, and it is a vulnerability we need to address.

Mr. MCCAUL. Dr. Romine, I guess from what I am hearing from you is that we don't want to get this wrong. I think Mrs. Watson Coleman was talking about herself being possibly in this pool of candidates that could get somehow mischaracterized. I mean, tell us where are we right now with the technology? How accurate is it?

Mr. ROMINE. How accurate is it, oh, I see. The very best algorithms that we have tested the most recently have false negative rates that are extremely low. The accuracy can range into the—for the best algorithms in a one-to-many match—can range into the 99.7 range.

Mr. MCCAUL. So 99.7 percent accuracy?

Mr. ROMINE. Accuracy.

Mr. MCCAUL. That is pretty good.

Mr. ROMINE. I beg your pardon?

Mr. MCCAUL. That is a pretty good number.

Mr. ROMINE. From a scientific standpoint, we report the number. The judgment on what is a pretty good number is up to the policy makers, but it is a high number for me.

Mr. MCCAUL. It is very high. You are a scientist, I am not, but it sounds pretty high to me. I think it is always a balance in this committee and when we deal with security issues, you know, we deal with privacy and civil liberties, we always have to balance these as Americans, and I think it is important that we balance

those factors. But I wouldn't want to throw the baby out with the bath water. I think the BITMAP Program has been extremely successful, has stopped a lot of bad actors from coming into the United States, and Mr. Chairman and Ranking Member, I hope that this committee, we could still advance that authorization and that bill through this Congress because I do think it is important to protect the American people. It is one of the most important responsibilities that we have as Members of Congress.

With that, I yield back.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the gentle lady from New Mexico, Ms. Torres Small, for 5 minutes.

Ms. TORRES SMALL. Thank you, Chairman. Last month, the CBP announced that there was a data breach with some of the subcontractors operating at land ports of entry along the Southern Border, and as a result, thousands of license plate numbers and images of drivers were taken, and images of drivers that were taken by facial recognition technology were compromised. I represent multiple border towns, where you cross back and forth into Mexico for jobs, shopping, tourism, medicine.

Also, within the interior of the district, there are border checkpoints, and when they are operating, that same information is being taken—license plates and facial—and pictures of people's faces. So we want to be able to make sure that the citizens' data is secure. Were there audits into the subcontractor's system prior to the hack?

Mr. WAGNER. I am not aware of that. I don't know. I will have to check.

Ms. TORRES SMALL. Can you get back to us on that, please? Thank you.

And did these private subcontractors have the authority to store those U.S. citizens' data?

Mr. WAGNER. They did not have the authority to have the pictures taken by the camera, from what I understand.

Ms. TORRES SMALL. Oh, so not even to store it, they did not have the authority to take any pictures of faces?

Mr. WAGNER. They had the authority to take them. They did not have the authority to take it off the camera and put it onto their own network, which is apparently what happened.

Ms. TORRES SMALL. They did. OK. What protocols did CBP have in place to oversee contractor and subcontractor data security practices?

Mr. WAGNER. I mean, they go through background checks. They are vetted. They are cleared. They are trained on use of the systems that they are going to work on. As far as having the audit controls on—this was a stand-alone pilot, so it was outside of our normal network, and we apparently did not have the same level of controls and audit capabilities on that, because it was a stand-alone, closed system. Those are things being put into place now on all those systems to make sure you can't connect a portable media drive on that and extract information. You know, our main network has these protocols on them, but we didn't have them on this type of system.

Ms. TORRES SMALL. So did you say those are in place now? You have corrected the problem?

Mr. WAGNER. They are being put into place now.

Ms. TORRES SMALL. They are being put into place now?

Mr. WAGNER. Yes.

Ms. TORRES SMALL. Can you follow up and let us know when they are in place?

Mr. WAGNER. Absolutely, yes.

Ms. TORRES SMALL. Because that is something of deep concern. Thank you.

With all pilot programs, because I remember going through the border checkpoints and being told, you know, this is a pilot, so don't worry about it yet——

Mr. WAGNER. Right.

Ms. TORRES SMALL. It is just a pilot. That is actually when we need to make sure that we are operating it correctly.

Mr. WAGNER. Agreed.

Ms. TORRES SMALL. So I want to switch now to Congressional authorization.

Mr. Wagner, it is my understanding that it is the law that Congress is enacting a biometric entry-exit system limit data collection to foreign nationals. Is that correct?

Mr. WAGNER. Yes.

Ms. TORRES SMALL. OK. Under what authority is CBP collecting biometric information on U.S. citizens as part of the entry-exit system?

Mr. WAGNER. We are using the information under 8 U.S.C. 1357B and 8 CFR 235.1, which allows us to consider any information or evidence pertaining to a person crossing the border in establishing their U.S. citizenship. So, generally, a person will present a U.S. passport to us. We can look at it. We can manually review. We can ask them questions how they obtained it.

Ms. TORRES SMALL. Thank you. Actually I am going to switch direction really quickly. I apologize. I know some of that was already covered, so I appreciate it.

I want to switch to the Federal agencies that are scanning through U.S. citizens' driver's licenses, and ICE is one of those that has been identified as potentially scanning through these databases. For what purpose—or are your components currently attempting to or successfully accessing State driver's license databases in any way?

Mr. WAGNER. So, for the biometric program we are discussing, we are not using driver's license information. We do use driver's license information from the States that have entered into agreements with us, where their driver's license also substitutes for a passport to cross the border. I think we have about 5 U.S. States and maybe 4 Canadian provinces that entered into written agreements with us to mark the citizenship of the driver's license holder on the document, so they can cross the border without having to go get a passport. That serves in lieu of the passport.

Ms. TORRES SMALL. Does the DMV in those States require probable cause or warrants to access that information?

Mr. WAGNER. Well, when that person crosses the border, our agreement allows us to verify with them that that is a valid license

and to retrieve the photo from that so we can see who it belongs to. We also have other law enforcement access through—into biographical driver's license data that we also might use in a law enforcement context that is very common for law enforcement agencies to access.

Ms. TORRES SMALL. Thank you, Mr. Wagner.

Chairman THOMPSON. Thank you very much.

The Chair now recognizes the gentleman from New York, Mr. Katko, for 5 minutes.

Mr. KATKO. Thank you, Mr. Chairman, and thank you all for being here today.

Just take a step back for a moment. As a Federal prosecutor for 20 years routinely dealing with homicides and matters of violent crime, some of the tools in the toolbox I had were fingerprints at first and, later, DNA.

When they both came on-line, at first there were concerns about how they would be used, and now they are becoming more mainstream. I hope and pray that it is the same with facial recognition.

But, you know, all three have the capability not only of helping to solve crimes but also making sure that crimes aren't committed. But even something we don't think about enough is exonerating people who are falsely accused. I mean, look at what the DNA system has done for people falsely accused in prisons. It has been a remarkable breath of fresh air.

So my concern is not with the efficacy of using it. My concern is that we get it right. Like we have done with fingerprints and like I think we are doing with DNA.

So my questions focus on the accuracy and the things we need to do to make it better. My colleagues have asked some great questions about the use of it and the extent of the use, and we are going to have to have more discussions about that. I am very concerned about the accuracy.

That was a big thing with DNA starting out, and now DNA is—the accuracy in the testing is amazing. It is almost—it is dispositive almost all the time. I don't think we are there yet with facial recognition. I would like to get there.

So, with that in mind, I want to ask Mr. Romine a couple of questions. You talk about the fact that you are charged with examining the gaps and limitations of certain things, including facial recognition.

So what do you see as the gaps and limitations of it right now?

Mr. ROMINE. The principal gaps and limitations we see involve a couple of things. One is image quality. It is still true garbage-in/garbage-out for software systems. So image quality has a huge impact.

We see—as I said, I will have a report on demographics, and there are certain issues associated with demographic effects. That is particularly true when you are trying to identify someone when you have a reference image that is maybe 10, 20 years earlier than the person that you are trying to identify. That can be a very big challenge.

Similarly, if someone has been injured or there is some obscuring of the face for other reasons, that can have a challenge.

Images that are taken noncooperatively. I don't mean uncooperative. I mean, where someone is not standing still looking at a camera with the intent of registering an image. If you are taking an image through a windshield, for example, or if you are taking an image of someone who is walking and not facing a camera, those can have a significant impact on the accuracy and the ability of these systems to do identification.

Mr. KATKO. OK. What can we do to improve that portion of it?

Mr. ROMINE. The industry continues to make advances. I mentioned the emergence of convolutional neural networks as a game-changer in this space. I think we don't know what we don't know coming down the pike, but I think there continue to be improvements that we see in our testing over time. So the industry is making great strides.

Mr. KATKO. You mentioned also, in response to a question from one of my colleagues, that the demographic effects of facial recognition software are diminishing.

Could you expound on that and what you mean by that? Because you say it is 99.7 percent accurate. But it is probably not 99.7 percent accurate for certain segments. So like, for example, darker-skinned female, I want to know what you are doing to make that better and how we can make it stronger.

Mr. ROMINE. That is correct. From NIST's perspective, what we do to make things better is provide an evaluation capability. So we are not doing any training——

Mr. KATKO. That is understood.

Mr. ROMINE [continuing]. Development. However, I would say that anytime the overall performance of the system improves as dramatically as facial recognition has improved over the last 5 to 6 years, the compression—the effect of differences in demographics shrinks as well. And the report later, once we have finished our analysis, the report that comes out in the fall, will——

Mr. KATKO. That sort-of answers my question. But you admit that certain demographics have a disproportionate error rate. So you are saying it is improving. How much has it improved?

Mr. ROMINE. We haven't finished the analysis yet, so I am not able to answer that question currently. The report will come out in the fall.

I will say that the—it is unlikely that we will ever achieve a point where every single demographic is identical in performance across the board, whether that is age, race, or sex. But we want to know just exactly how much the difference is.

Mr. KATKO. This report will detail that when it comes out in the fall?

Mr. ROMINE. Yes, sir.

Mr. KATKO. All right. Thank you very much. I yield back, Mr. Chairman.

Chairman THOMPSON. We all look forward to the report.

Mr. KATKO. Indeed.

Chairman THOMPSON. I assure you.

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

Ms. UNDERWOOD. Thank you, Mr. Chairman.

Mr. Gould, I represent Illinois' 14th District, where we drive about an hour or two to get to major airport in Chicago. So our community is always interested in learning more about the technologies that can potentially improve security at airports while still reducing the flier's wait time.

However, before implementing any new technologies, like biometric screening, it is really important, crucial even, to make sure that they are proven to be effective, reliable, and fair.

So can you please run through the ways in which TSA is currently employing biometric screening at checkpoints?

Mr. GOULD. Yes, ma'am.

Currently, we are only using biometrics technology in the international terminal, Terminal F, in Atlanta. That is on a pilot basis.

Our approach to biometrics implementation at TSA is extremely deliberative. We want to understand how the technology works, how it can improve identity verification for the traveling public, and how it can improve the passenger experience.

Going back to the discussion on image quality that happened before, we are in a fortunate case at TSA in that we really control the environment in our checkpoints so we can ensure optimal lighting, optimal distance from the camera, so we get the highest quality images possible for biometric matching. For the pilot in Atlanta, we are matched up with CBP using their TVS system, and we see extremely high match rates there.

Moving forward, we will look to pilot 1-to-1 matching capability where a traveler will provide a credential, that credential will be assessed by our CAT machine, and it will return a match rate on whether or not the face that has been captured matches the face that is embedded in that credential.

In that scenario, no information even leaves the checkpoint and nothing is retained on the camera. So that is some of the things that we are looking at. I believe that, when we are through with, you know, these pilots that we are doing for biometric development, we will see that we cannot only improve passenger security but also make it a much more positive experience for the traveling public by reducing wait times.

Ms. UNDERWOOD. That is great.

How are the airports and airlines using the biometric security screening technology beyond the TSA checkpoints, if you are aware, and what other uses are planned for the future?

Mr. GOULD. So, right now, I can comment on really what we are doing in Atlanta with Delta Airlines.

Ms. UNDERWOOD. OK.

Mr. GOULD. In Atlanta, the Delta Airlines kiosks use biometric identification when the passenger checks in, to make sure—should they choose to do so—to make sure that that person is the passenger who is ticketed on that particular flight.

TSA has oversight of the bag drop to ensure the passengers are positively matched to bags in the international—you know, for international travel. So Delta Airlines has a security program amendment that we have granted them to use biometric technology to do that matching at the bag drop.

We use it at our checkpoint in Atlanta. Then it is, of course, subject—it is used at the exit point, at the gate.

Ms. UNDERWOOD. OK. So is that the only specific agreement with an airport or airline that TSA has to govern the use of biometrics? So you said——

Mr. GOULD. Right now, the security program amendment that we have granted Delta for the limited use only in Atlanta is the only formal agreement that we have entered into with the airlines.

Ms. UNDERWOOD. So does TSA have any role in improving airport and airline uses of biometric technology?

Mr. GOULD. We have roles in improving the use of biometric technology where TSA has equities. Again, I would go back to say that would be the checkpoint and the bag drop. So, if an airline wanted to use biometrics at the bag drop to positively match that traveler to that bag, they would have to request a security program amendment, and we would have to issue it.

Ms. UNDERWOOD. OK. As the use of biometric data continues to expand, Illinoisans understandably have a lot of questions about how such sensitive personal data is used and stored.

So I would like to open this question up to the panel.

Under what circumstances do your components collect biometric data on U.S. citizens?

We can start with Mr. Wagner.

Mr. WAGNER. You say collect on U.S. citizens?

Ms. UNDERWOOD. Yes, sir.

Mr. WAGNER. We are temporarily holding it while we validate that it corresponds to the passport that person is presenting, and then it is purged after 12 hours from our system.

Ms. UNDERWOOD. OK.

Mr. GOULD. From a TSA perspective, we are leveraging photographs that travelers have provided to facilitate travel like passport photographs. When we capture the image at the checkpoint, it is not retained at the camera. Once that image is encrypted and transmitted, we only get back a match result.

Ms. UNDERWOOD. Interesting. OK.

Mr. DI PIETRO. Ma'am, Secret Service collects fingerprints, palm prints, mugshots, other identifying information on individuals who we arrest as part of our criminal investigations.

Ms. UNDERWOOD. But not as part of regular screening?

Mr. DI PIETRO. Pardon?

Ms. UNDERWOOD. You don't retain the data that you collect as part of the regular screening?

Mr. DI PIETRO. That is correct.

Ms. UNDERWOOD. You don't store it?

Mr. DI PIETRO. No, no. Regular screening, we use metal detectors, cabinet X-rays, things like that cap.

Ms. UNDERWOOD. And fingerprints. So to get into the White House——

Mr. DI PIETRO. No, we do not use fingerprints at the White House. We don't scan for that.

Ms. UNDERWOOD. Great.

Yes, sir?

Mr. ROMINE. The data that we have is sequestered in servers that are air gapped—they are not connected to the internet—in a locked door. I am the director of the laboratory, and I am not per-

mitted to go into that room without being escorted. So it is very tightly controlled.

Ms. UNDERWOOD. Thank you so much.

I yield back.

Chairman THOMPSON. Thank you.

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

Mr. WALKER. Thank you, Mr. Chairman.

Ninety-nine-point-seven percent, that is pretty good, or about ironically the same on-base percentage that Cedric Richmond has at our annual baseball game, but that is another topic. A problem, I should, say not a topic.

But I do have a question for you, Dr. Romine.

How do you ensure—and I think Ms. Underwood was just kind-of approaching this. How do you ensure that the biometric data collected is secured?

Let me unpack a little bit more. Is the biometric identifier connected directly to other possibly sensitive or private information about the person?

Mr. ROMINE. The data that we have on facial recognition is not connected to identifying information. So I will have to double check the exact features there, but I am——

Mr. WALKER. Can you do that for us and report back?

So you are saying that the information that you are collecting is secured?

Mr. ROMINE. The information we are collecting—we don't collect information. We obtain it from our partners for the purposes of evaluation only, and we secure that in—it is in a secure server.

Mr. WALKER. Let's use the word "obtain" instead of "collect."

Have you ever had a breach on the information you have obtained?

Mr. ROMINE. No, sir.

Mr. WALKER. OK. Thank you.

Questions for the panel. Keep it about 10 or 15 seconds will be good. That way we can get everybody in here.

Can you elaborate more on these programs that have been successful, specifically on the ones identifying facial recognition, any other biometric technologies? If you can elaborate either on the success of them or adding security benefits or expediting travel for passengers?

We will start with Mr. Wagner.

Mr. WAGNER. Sure. It gives us the ability to validate a person's biographical identity within 2 to 3 seconds without having to handle the physical passport and allows us to link it up in a secure way. So the person we did all our National security checks against in TSA, international security checks on international flights, corresponds to the person who is in front of us.

Mr. WALKER. Mr. Gould.

Mr. GOULD. Sir, with our pilot in Atlanta, we do data collection on the number of people who were choosing not to provide biometric identification at our checkpoint, and it was less than 1 percent. People seem to enjoy it. The traveling public moves through the checkpoint very rapidly. The best part of it is we enhance identity verification, thereby enhancing security.

Mr. WALKER. OK. Mr. Di Pietro, does it impact you at all?

Mr. DI PIETRO. Not really. Right now, we are piloting some technology, but we are in the middle of that test right now, so we haven't compiled the data. The tests will finish up at the end of August, and then we will have a chance to go through and review the data, and then we will be able to draw some conclusions. But at this point, we are still in the middle of the test.

Mr. WALKER. Dr. Romine, anything there?

Mr. ROMINE. No, sir.

Mr. WALKER. OK. Going down the panel again.

Based on these successes—specifically Mr. Wagner and Mr. Gould—where do you see the use of biometric technologies expanding in your specific agency, even beyond a complete roll-out of the pilot programs?

Mr. Wagner.

Mr. WAGNER. It will significantly transform the arrivals and departures on international travel in all our different environments, air, land, and sea, and can really build a very convenient, efficient, facilitative but yet secure process for us to do that.

Mr. WALKER. Mr. Gould.

Mr. GOULD. Sir, so for us, we will build on the success of our international partnership with CBP that we are doing in Atlanta to other international travel locations. We will look to use the CBP system for our trusted traveler population—PreCheck, Global Entry—to do one-to-few or one-to-many matching for biometrics purposes at our checkpoints.

Then really the next step that we are looking at is that 1-to-1 matching that I mentioned before, where a traveler can approach the checkpoint, provide a credential, have the CAT machine, credential authentication technology machine, assess the image embedded in that credential and then match it to a photograph that is taken right there.

Mr. WALKER. All right.

Mr. Di Pietro, do you ever share your information with local or State governments?

Mr. DI PIETRO. Information with respect to fingerprints?

Mr. WALKER. Information that you collect. Let me back up and ask this question, because I think I have got time to get it in. Ms. Underwood asked a couple of questions, and there seemed to be just a touch of hesitancy, so I wanted to follow back up there.

The data that you collect, is it ever collected without subjects being aware?

Mr. DI PIETRO. No, sir.

Mr. WALKER. OK. All right. So the information that you do collect, fingerprints, et cetera, do you ever share that with State or local?

Mr. DI PIETRO. I would have to check with our lab director on that, sir, and get back to you.

Mr. WALKER. Are you familiar with any circumstances that you have in the past?

Mr. DI PIETRO. Sir, I am the Secret Service's chief technology officer. I work more on the engineering and technical side. I would have to get with our Forensic Services Division to answer that.

Mr. WALKER. Fair enough. I thank you for your time.

I yield back, Mr. Chairman.

Chairman THOMPSON. Just let me comment.

In a Classified setting, we are going to ask that question again of the data collected that people don't know, because I think there is information being collected in the pilot at the White House that is different from the answer. But we plan to have a Classified briefing on that issue.

The Chair recognizes the gentlelady from New York for 5 minutes, Ms. Clarke.

Ms. CLARKE. Thank you, Mr. Chairman.

Some would say let's not make—when it comes to National security, let's not make the perfect be the enemy of the good. But, unfortunately, the good is not good enough when bias is baked into the algorithms that create false positives. The stakes are far too high for individuals and too costly, particularly for women and people of color.

The wide-scale deployment of facial recognition technology will have profound implications on privacy. We must look before we leap. It is imperative that Congress impose safeguards against mission creep and ensure biased algorithms do not make their way into wide-spread use.

As a New Yorker, one who lives just miles away from Ground Zero, National security is crucially important. I know that firsthand.

But facial recognition technology that routinely misidentify women and people of color don't make us safer; they make us less safe. Using this technology to help ICE target immigrants for deportation doesn't protect us from terrorism; it terrorizes hardworking families. When CBP uses these technologies on U.S. citizens traveling abroad without providing a transparent opt-out process, that is potentially unlawful.

We have seen what happens when technology is widely deployed before Congress can impose meaningful safeguards. Let's not make the same mistake with facial recognition technology.

You have a contractor that has a breach, and we know that we are seeing more use of video; deep-face, if you will. That information gets in the hand of an adversary overseas, and they want to create a disruption in our Nation, all you have to do is take that information, create a video from it, and, bam, we are already into a really bad situation.

I don't know if we are looking at the interconnectedness of all of these technologies, particularly because they are all evolving. I am very concerned about the lack of specificity that we have at this stage.

So my question is about accuracy. Mr. Wagner, CBP boasts that the facial recognition algorithm it uses is able to make a match of 98 or 99 percent of the time. But that statistic does not include instances where facial recognition technology is unable to capture a high-quality image due to human error, poor lighting, or other environmental factors.

Recent testing by the DHS science and technology director has shown that, when data capture factors are included, the error rate increases to around 10 percent.

Do you dispute S&T's findings?

Mr. WAGNER. No.

Ms. CLARKE. OK. Why does CBP insist on tracking a bogus statistic that ignores passengers who cannot be photographed well enough by the system to be matched?

Mr. WAGNER. What we are accounting for is, if we take a photograph that is of sufficient quality, are we able to match it.

Ms. CLARKE. If?

Mr. WAGNER. Correct.

Ms. CLARKE. OK.

Mr. WAGNER. Then we know we need to address the camera itself and the lighting conditions to make sure that we are capturing 100 percent of those photographs that we can then match at the 98 to 99 percent. Two separate statistics. They are both valuable to us.

Ms. CLARKE. Yes. There is also the false positive, the cost of the false positive. That individual that is detained for whatever reason because there is a false positive, the cost of that person's health, the cost of that person's well-being, perhaps there is a commerce concern involved. I am concerned about the lack of accuracy. I am very concerned about the lack——

Mr. WAGNER. If the person doesn't match the photo in this case, they present their passport as they are doing today.

Ms. CLARKE. Excuse me?

Mr. WAGNER. If a person doesn't match a photograph, they simply present their passport and their boarding pass.

Ms. CLARKE. If they trying to match them and they don't match, what happens to that individual?

Mr. WAGNER. They present their boarding pass and their passport——

Ms. CLARKE. Uh-huh.

Mr. WAGNER [continuing]. And it is manually reviewed at that point in time, just as happens today.

Ms. CLARKE. Is that—and those people are not detained in any way? They are not asked to step aside, they are not asked—the process does not delay that person?

Mr. WAGNER. No. They just show their passport.

Ms. CLARKE. OK. I hope that is the case.

Will CBP commit to tracking a more meaningful statistic that captures the usefulness and accuracy of the full facial recognition process, including the rate at which the system fails to capture a quality image?

Mr. WAGNER. We do track those rates. We track the—what we call the gallery completion rate. We are never going to have 100 percent of a gallery because not everybody needs a passport to travel.

Ms. CLARKE. Including the images that are not high-quality, those that fail to meet your standard?

Mr. WAGNER. Right. We want to build it so that the camera will take a high-quality photograph.

Ms. CLARKE. I know that is what you want to do. But will you be keeping statistics on what doesn't meet that standard?

Mr. WAGNER. So we are, correct, yes.

Ms. CLARKE. Very well.

I yield back, Mr. Chairman.

Chairman THOMPSON. The Chair recognizes the Ranking Member.

Mr. ROGERS. Thank you, Mr. Chairman.

I just want to clarify with the Secret Service: The information that you have collected in this pilot program that you talked about earlier, is it my understanding that everybody that is in that are employees of the Secret Service, and they volunteered to be in it?

Mr. DI PIETRO. That is correct. Maybe if I can explain how we are doing the pilot, that might help.

Mr. ROGERS. Also, when did the pilot start?

Mr. DI PIETRO. So we published the PIA back in November, it began in December, and it is going to run through August. We did that on purpose. We wanted it to go from the winter into the summer because of the different items people wear, so that we have a good amount of time where we were assessing it.

Maybe if I just explain a little bit of how the pilot is working, that might help explain this for you.

As you indicated, the participants of the pilot are Secret Service employees who volunteer to take part in this effort. The facial images are stored when associated match is recognized on an individual, on one of the volunteers. At the conclusion of the pilot, all of that information will be deleted.

We are using our current CCTV system, video management system we have at the White House. I can imagine you have got a similar system up here on Capitol Hill that you use for CCTV surveillance. We are using those video feeds there, and we are trying to match the individuals that are in the pilot, the volunteers, to the people who we are seeing in those cameras. If there is no match, there is no record. If there is a match, then there is a record. That will be retained till the end of the pilot, and then that information will be deleted at the conclusion of the pilot.

Mr. ROGERS. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you. But I think Mr. Katko's question was, if you were collecting data, capturing data, and you said no. My question is, whether it is a volunteer or a person walking the street, you are collecting data?

Mr. DI PIETRO. That is correct. That is right.

Chairman THOMPSON. The Chair now recognizes the gentleman from Louisiana, Mr. Higgins.

Mr. HIGGINS. Thank you, Mr. Chairman.

Director Romine, would you describe biotech—biometric technology and facial recognition technology as designed to work with trained agents? In other words, man and machine working together? Is this what this is working toward?

Mr. ROMINE. We are agnostic as to whether that is the use case or not. But our testing has verified that, in the case of facial recognition, the best algorithms and the best human face recognizers, the trained face recognizers——

Mr. HIGGINS. I thank you for pointing that out. In your testimony, NIST has researched in an effort to measure the accuracy of forensic examiners, including forensically-trained facial reviewers.

Mr. ROMINE. That is correct.

Mr. HIGGINS. Your statement stated that it presented data comparing state-of-the-art facial recognition algorithms with the best human face identifiers, the best machines performed in the range of the best performing humans——

Mr. ROMINE. That is correct.

Mr. HIGGINS [continuing]. Who are professional facial examiners. But you went on to state that optimal face identification was achieved only when humans and machines collaborated.

Is that an accurate assessment?

Mr. ROMINE. That is correct.

Mr. HIGGINS. Let me ask, Commissioner Wagner, is there ever an arrest made or denial to travel based solely on facial recognition technology?

Mr. WAGNER. No.

Mr. HIGGINS. Thank you.

So facial recognition technology gets a—let's call it a hit, a high probability based on algorithms, that a particular traveler is a person of interest. Then an agent looks into the documentation further and has personal interaction with that individual, which then approves the individual for travel or prompts further and deeper investigation. Is that correct?

Mr. WAGNER. Yes, that is correct.

Mr. HIGGINS. So, just to clarify for America watching, this technology is being used to enhance the efficiency and the speed by which the trained agents can move travelers through screening points. Is that contract?

Mr. WAGNER. Yes.

Mr. HIGGINS. Thank you for clarifying that.

Is the general consensus amongst travelers and airlines that this technology is a good idea, is working well?

Mr. WAGNER. I believe so, yes.

Mr. HIGGINS. Thank you for clarifying that.

Let me jump into your data breach. It is a concern for all of us, regardless of which side of the aisle we are on.

Who reported that breach? Did they self-report, or was it discovered? How was it discovered? Is my first two questions about that. Who reported it, the contractor, or did you all discover it?

Mr. WAGNER. No. I believe we asked them about it.

Mr. HIGGINS. How much time went by?

Mr. WAGNER. A significant amount of time. I need to verify this, but my recollection seems to be that we asked them if any of our data was included in it, and they came back and said yes.

Mr. HIGGINS. Not to put you on the spot here, my brother, but I am going to. When you say an amount of time, a pretty significant amount of time, are you talking days, weeks, months?

Mr. WAGNER. I have that answer. Let me look for that, and I will come back to you.

Mr. HIGGINS. OK. We would like to know that, because it is—the contract was referred to as subsequently terminated. We would like very much to know what the course of events were regarding—what was the time line here with this contractor from the time the breach happened till the time it was discovered and inquired about and reported and verified, and then how much time before that contract was terminated?

I believe—I would like to know, and perhaps my colleagues would like to know, if that contractor is still on the contracting list? If that contract was terminated with that contractor, but are they still out there bidding on other contracts? I believe we would like to know that.

Commissioner Wagner, you have a tremendous job to do.

You, gentlemen, thank you for your service, all of you. It is important to the Members of this committee to get things right.

Many ports of entry, particularly land ports, face unique challenges implementing the biometric entry/exit system.

Can you just share what—this is my final question—what are the primary challenges and how can we help?

Mr. WAGNER. The primary challenge was finding a way to implement this into a travel system that wasn't designed to support the, say, collection of biometrics on only a segment of the traveling public.

You know, unlike Europe and Asia and other places, we don't have departure controls. You don't see a CBP Officer to get your passport stamped to depart the United States. We have never restricted departures like that. So international flights comingle with domestic flights. Then with each individual flight, you have got U.S. citizens, permanent residents, and visitors. So how do you sift and sort and differentiate between who is in scope or out of scope of the biometric exit requirement, what technology do you use to collect that biometric, and how do you ensure a way that is not going to create gridlock at the airports or the seaports or the land border, when we get to it, on how to do that.

Mr. HIGGINS. That is exactly what you are working through right now, correct?

Mr. WAGNER. Right. So we found a way using the facial recognition and compare people against data they have already provided in a convenient, quick, and accurate way that we can apply to all travelers using different authorities and help the airlines board the planes even faster.

Mr. HIGGINS. Mr. Chair——

Thank you for that answer.

My time has expired, Mr. Chairman.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the gentlelady from New Jersey for 5 minutes, Mrs. Watson Coleman.

Mrs. WATSON COLEMAN. Thank you, Mr. Chairman.

Thank you, gentlemen, for your testimony. This is a very, very important issue for us. I mean, we want to be safe and secure, but we also want to recognize that our privacy is our privacy, and we have guarantees under the Constitution and that we are not in any way infringing upon that.

Mr. Wagner, I would like to ask you a question. I understand the Department has sent an interim final rule to OMB that would expand CBP's collection of biometric data, something we have obviously expressed tremendous interest in.

The committee is eager to learn as much as possible about what you intend with this rule and why you haven't pursued a more transparent and deliberative process.

What does this interim final rule entail, how does it address CBP's collection of biometric data on U.S. citizens, and why did you choose this closed process rather than providing notice and allowing public comment?

Mr. WAGNER. There are several pieces of rulemakings underway. There is an interim final rule that is drafted and is circulating through the Government for comment. There is also notice of proposed rulemakings on other parts of what we would like to propose to do. We are evaluating all of those right now based on a lot of the comments we have received back from within Government, and we may take a different approach.

There are regulations in place already, though, concerning biometric exit that have been in place that we are utilizing today. Through the privacy impact assessments, we have explained in great detail—in greater detail than would be in the regulations probably even—how the program operates and what exactly what happens with it. That is publicly available.

Mrs. WATSON COLEMAN. Are you having conversations with stakeholders?

Mr. WAGNER. Absolutely. I have personally done meetings with—two different meetings, the East Coast and West Coast, with the privacy community and all of the privacy representatives. We are certainly talking with all of our travel and tourism stakeholders. There is vehement support behind this in the travel and tourism arena. Of course, we are talking with the airlines and airports and our Government partners as well.

Mrs. WATSON COLEMAN. Why is it that I am asking you this question about why the committee doesn't have the information it needs? If these discussions have been in the public realm, why am I asking you about this process? What part of this process fits this question about why you have chosen to do it in a more closed way as opposed to a more transparent way? Or am I just misunderstanding and just misstating?

What part of your consideration, your rulemaking request, your request to OMB, don't fit this sort of public sharing?

Mr. WAGNER. I am not sure I understand the question.

Mrs. WATSON COLEMAN. Well, according to the information that I was given, the Department has sent an interim final report to OMB. This interim report has to do with expanding your collection of biometric data and that the process that you all are using in dealing with OMB has been a closed process.

What does that mean?

Mr. WAGNER. So there are certain provisions that would be in the interim final rule that, if OMB were to approve it, we could publish that in the *Federal Register*. You can still accept comments, I believe, on that, but the rule goes into effect.

Really that——

Mrs. WATSON COLEMAN. What is the problem with there being a more open process now as——

Mr. WAGNER. We are doing that, too, for the other provisions.

Mrs. WATSON COLEMAN. Well, what about the provisions—I am specifically asking about the provisions that you are not doing it on. What is the reason for that?

Mr. WAGNER. I am——

Mrs. WATSON COLEMAN. Alright. So have you a number of proposals, rulemaking proposals——

Mr. WAGNER. Correct.

Mrs. WATSON COLEMAN. Right?

Part of this, the Department has sent a final—an interim final rule to OMB. In this particular rule, it deals with the expansion of CBP's collection of biometric data.

The understanding that I have been given is that the process that you are engaging in is a closed process, and we don't have—the committee doesn't have the benefit of what is being considered, what you are asking for. Instead, you have used another process that forecloses that opportunity.

So I am asking, why would you choose to do that? What is it that you are asking for that you can't share in the asking? Not after the fact.

Mr. WAGNER. Well——

Mrs. WATSON COLEMAN. Or is there not such a thing, and we are just completely uninformed?

Mr. WAGNER. No. It is just the different portions of rulemaking process. Before the rule is even finalized, it would be premature to talk about what is in it or what is not in it, because that is going to change. Based on the feedback and our discussions with OMB, it is going to change.

Mrs. WATSON COLEMAN. But you do that on other rulemaking requests, but not on this specific area?

Mr. WAGNER. We will be publishing a notice of proposed rulemaking with anything that would fall within those parameters.

Mrs. WATSON COLEMAN. It is somewhat frustrating——

Chairman THOMPSON. What I think the point is, at this point, the public has no input in this process, as far as we understand.

Mrs. WATSON COLEMAN. Yes.

Chairman THOMPSON. The rulemaking process.

Normally the notice for rulemaking——

Mr. WAGNER. Right.

Chairman THOMPSON [continuing]. You push it out and receive comment.

Mr. WAGNER. We will do notice of proposed rulemakings to solicit that feedback.

Chairman THOMPSON. You will?

Mr. WAGNER. We will.

Mrs. WATSON COLEMAN. OK. After that.

Chairman THOMPSON. We finally got to where we—OK.

Mrs. WATSON COLEMAN. May I just have 30 seconds, since you so generously——

Chairman THOMPSON. I will give the lady an additional 30 seconds.

Mrs. WATSON COLEMAN. I am just sort-of curious about the Secret Service pilot project, and I wanted to understand—I understand that you are using this pilot project now with volunteer Service agents, so that when they are walking, you collect that information, if it matches, it works.

Are you incidentally collecting other information on people who are not part of this voluntary effort? If so, what are you doing with those sort of pictures that you capture?

Mr. DI PIETRO. So, ma'am, the cameras that we are using as part of this pilot are part of the White House video management system. That is the CCTV system that records videos from all of the cameras around the complex. We retain that data for 30 days as part of the CCTV process.

If we are—as we are going through and we are identifying those volunteers that are in there, that record is saved, and we save that and we are going to evaluate that to the end of the process.

Mrs. WATSON COLEMAN. But do you have the opportunity to review other—other faces that you are capturing that are in the vicinity, tourists, demonstrators, whatever?

Mr. DI PIETRO. If it would be something like a false positive, somebody who wasn't in our pilot but thought it was, that image would be retained in the——

Mrs. WATSON COLEMAN. We are concerned about what happens with——

Chairman THOMPSON. Part of—we will have a Classified briefing.

Mrs. WATSON COLEMAN. Thank you.

Chairman THOMPSON. We will have a lot of those questions responded to.

Mrs. WATSON COLEMAN. Thank you for your extension of time. Thank you very much for your——

Chairman THOMPSON. Thank you.

The Chair recognizes the gentlelady from Arizona, Mrs. Lesko, for 5 minutes.

Mrs. LESKO. Thank you, Mr. Chairman.

First, if you don't mind, I would like to yield a few seconds to my colleague, Mr. Higgins.

Chairman THOMPSON. 5 minutes.

Mr. HIGGINS. Thank you, ma'am.

Mr. Chairman, I ask unanimous consent to enter into the record 2 op-ed articles in support of law enforcement application of biometric technology.

The first is from New York City Police Commissioner James O'Neill, and the second is from managing director of the Chertoff Group, Lee Kair.

Chairman THOMPSON. Without objection.

[The information follows:]

HOW FACIAL RECOGNITION MAKES YOU SAFER

Used properly, the software effectively identifies crime suspects without violating rights.

By James O'Neill, June 9, 2019, New York Times.

In 1983, when I was sworn in as a police officer, many of the routine tasks of the trade would have seemed more familiar to a cop from my grandfather's day than to a new police academy graduate today. I took ink fingerprints on paper cards and used a Polaroid camera for mug shots. Reports were handwritten or typed on carbon triplicates. Biological evidence could be analyzed only in terms of blood type.

Technology has improved the profession beyond what the most imaginative officer could have conceived in those days. These innovations include facial recognition software, which has proved its worth as a crime-fighting resource since we adopted it in 2011. But the technology has also raised concerns about privacy, so the public should know how the New York Police Department uses its system—and the safeguards we have in place.

When detectives obtain useful video in an investigation, they can provide it to the Facial Identification Section, of the Detective Bureau. An algorithm makes a template of the face, measuring the shapes of features and their relative distances from

each other. A database consisting solely of arrest photos is then searched as the sole source of potential candidates—not photos from the Department of Motor Vehicles, Facebook, traffic cameras or the myriad streams of closed-circuit TV video from around the city. Facial "landmarks" are compared without reference to race, gender or ethnicity.

After the software generates a list of possible matches, an investigator assesses their resemblance to the suspect. If one is selected, a review is conducted by detectives and seasoned supervisors, noting similarities and differences. If they affirm the match, the investigator proceeds with further research, including an examination of social media and other open-source images.

We might find social media images of a person at a birthday party wearing the same clothing as the suspect in a robbery. That person then becomes a lead; the facial identification team will provide only a single such lead to the case detective. Leads provided by the unit are comparable to tips to our Crime Stoppers hotline—no matter how compelling, they must be verified to establish probable cause for an arrest. No one can be arrested on the basis of the computer match alone.

In 2018, detectives made 7,024 requests to the Facial Identification Section, and in 1,851 cases possible matches were returned, leading to 998 arrests. Some investigations are still being conducted and some suspects have not been apprehended.

But in many cases there have been clear results. Recently, the work of the facial identification team led to the arrest of a man accused of raping a worker at a day spa, and another charged with pushing a subway passenger onto the tracks. We have made arrests in murders, robberies and the on-air assault of a TV reporter. A woman whose dismembered body was found in trash bags in two Bronx parks was identified. So was a woman hospitalized with Alzheimer's, through an old arrest photo for driving without a license.

The software has also cleared suspects. According to the Innocence Project, 71 percent of its documented instances of false convictions are the result of mistaken witness identifications. When facial recognition technology is used as a limited and preliminary step in an investigation—the way our department uses it—these miscarriages of justice are less likely.

We have never put police sketches into the system; they would be of no value. We have used editing software to substitute a generic feature when a suspect is closing his eyes or sticking out his tongue in the submitted photo. The system can also create a mirror image of the right side of a face if we have only the left side, for example, to produce a 3–D model.

We use these methods solely to fill in missing or distorted data. And when we do so, we bring an additional degree of scrutiny to the process. To compare this to filling in a partial fingerprint, as the Georgetown Center for Privacy and Technology did in a recent report, is absurd. It makes sense to create an image of a suspect's left ear using his right ear as a model. But it is impossible to infer the shape of a nose from the shape of a chin. As the algorithm is constantly improving in its ability to read lower-quality images, the editing software is used less and less frequently.

The department does not conduct civil immigration enforcement, and neither does our Facial Identification Section. But we do work with other police departments when appropriate. A recent request from the F.B.I. led to the identification of a child sex trafficker who advertised his services on social media.

Biometric technology is no longer new. It is routinely used everywhere from shopping malls to doctors' offices. Its application by the department is carefully controlled and its invaluable contributions to police investigations have been achieved without infringement on the public's right to privacy. When cases using this technology have been prosecuted, our methods and findings are subject to examination in court.

Facial recognition technology can provide a uniquely powerful tool in our most challenging investigations: When a stranger suddenly commits a violent act on the street. In the days of fingerprint cards and Polaroid mug shots, these crimes defined New York City, for visitors and residents alike.

Though far rarer now, they remain life-altering, and sometimes life-ending, events. To keep New York City safe requires enormous and relentless effort. It would be an injustice to the people we serve if we policed our 21st-Century city without using 21st-Century technology.

James O'Neill is the police commissioner for New York City.

BIOMETRICS CAN PROTECT OUR BORDERS—ALONG WITH OUR PRIVACY

By Lee Kair, opinion contributor, 05/09/19 11 o'clock AM EDT, TheHill.com

Customs and Border Protection (CBP) has been expanding its biometric programs with the use of facial recognition technology for inbound passengers, achieving early success both in identifying imposters attempting to enter the U.S. and improving the efficiency of the screening process itself.

Based on this success, the Department of Homeland Security (DHS) recently announced efforts to expand programs to those departing the U.S., with the goal of covering 97 percent of outbound international travelers in the next 4 years.

As DHS applies facial recognition and other biometric technologies to confirm travelers' identities and to intercept potential threats, it is important to look at how it balances travelers' privacy with security goals.

Not surprisingly, the expanded use of biometrics raises questions about individual privacy, particularly in light of proliferating, high-profile data breaches that can affect—and should alarm—all of us.

As the lead agency for protecting our nation's borders, CBP has evolved its process for identifying and screening passengers over time. In "the old days," passengers flying into the United States would present their passport to a CBP officer. The officer compared the laminated picture within the passport to the person standing in front of them, researched available government data sources to determine if the traveler was high-risk, and conducted in-person interviews to determine if additional screening was necessary. Although a sufficient process, it was time-consuming and dependent on CBP personnel to make accurate assessments and detect anomalies in real time.

Since 2005, CBP has required airlines to provide manifest data shortly after departure so officers can leverage existing targeting infrastructure and resources, including government documentation and photographs (such as passport and visa photos), to determine the risk of incoming passengers before they arrive. Upon landing, low-risk passengers are expedited through customs while CBP focuses its resources on higher risk passengers.

Today, CBP is leveraging commercially available biometric technologies to streamline and automate the existing process of manually matching images from data bases to individual travelers attempting entry into or exit from the U.S. The Transportation Security Administration (TSA) and aviation industry partners also are conducting biometric pilots across the country to expedite the traveler experience at the airport. These pilots are intended to confirm the identity of traveling passengers at various points in the airport ecosystem, with the goal of enhancing security while reducing friction in the travel process.

As stakeholders evaluate CBP's deployment of biometric technology, there are three areas where CBP has demonstrated best practices that meet the goal of promoting both security and an improved traveler experience. These include leveraging new technology for more efficient and effective screening; providing transparency around the collection and use of biometrics in the screening process; and voluntary opt-in or opt-out participation for other biometric programs:

Transparency.—CBP and TSA have issued several Systems of Records Notices and Privacy Impact Assessments while inviting public comment and publicizing strategies and roadmaps to educate and inform stakeholders on the steps they are taking to leverage technology for the security of the traveling public. This level of transparency is critical to developing trust between travelers and the government. In an era in which commercial companies often use "terms of service" obfuscated with pages of legal language, the government is being clear about its use of biometrics.

Leveraging existing systems to make them more efficient.—Where the government already had access to—and used—biometrics through existing systems (such as photos from passports, visas, previous border crossings or trusted-traveler programs), the use of matching technology expedites old manual processes. This speeds the traveler experience and is more effective than manual visual comparisons. For example, automated matching of a facial or fingerprint biometric at the TSA screening checkpoint is likely more accurate and faster than a security officer's visual driver-license check. These enhancements allow TSA to increase speed and security while reallocating officer resources to focus on detecting additional threats to aviation security.

Voluntary use.—CBP and TSA strategies also require the ability to opt in or opt out of other biometric matching programs and third-party use of biometrics. Specifically, CBP programs allow passengers to opt out of technical demonstrations as well as the sharing of biometric information with third parties (such as airlines); TSA requires opt-in participation for its biometric trusted traveler programs at TSA checkpoints.

Many privacy advocates are concerned that the government could use the data for continuous surveillance without any suspicion of wrongdoing, to identify and track people without their knowledge. Critics claim that it's an overreach for the government to require U.S. citizens to submit to facial scans to board a plane.

However, it is important to point out that CBP privacy policies only allow the biometric data to be used for identification purposes and that it must be deleted within 12 hours, in the case of U.S. citizens. Similarly, TSA is limiting its biometric programs to trusted-traveler programs, in which travelers have already chosen to share information.

In a time when we have seen rising concerns about stockpiling user data on social media, the use of biometrics by both the government and commercial entities must continue to be evaluated. Countries around the world are assessing the privacy exposure related to biometrics and facial recognition. The potential for commercial entities to combine biometric data with other user data—including geolocation, online activity and retail purchases—has the potential to significantly expose sensitive information about private citizens.

While DHS's pilot programs must be evaluated on a continuous basis, I believe that DHS has handled the implementation correctly. This should be the standard for other organizations and government entities looking to deploy biometric-based solutions that create a more secure, trusted environment for the public.

Lee Kair is managing director of The Chertoff Group, a security and risk management advisory firm. He served more than 15 years in senior executive positions at the U.S. Department of Homeland Security, including the Transportation Security Administration. The Chertoff Group is a frequent adviser to clients in the defense technology and aviation industries, including clients that work in identity management and biometrics technology. Follow on Twitter @ChertoffGroup.

Chairman THOMPSON. The gentlelady is recognized for the additional time.

Mrs. LESKO. Thank you, Mr. Chairman.

I, too, ask unanimous consent to enter into the record 3 letters expressing support for the effective and responsible use of biometrics by TSA and CBP. These letters are from Airlines for America, the International Air Transport Association, and the Global Business Travel Association.

Chairman THOMPSON. Without objection.

[The information follows:]

LETTER FROM SHARON PINKERTON TO CHAIRMAN BENNIE G. THOMPSON AND RANKING MEMBER MIKE ROGERS

July 8, 2019.

The Honorable BENNIE THOMPSON,
Chairman, Committee on Homeland Security, U.S. House of Representatives, 2466 Rayburn House Office Building, Washington, DC 20515.

The Honorable MIKE ROGERS,
Ranking Member, Committee on Homeland Security, U.S. House of Representatives, 2184 Rayburn House Office Building, Washington, DC 20515.

DEAR CHAIRMAN THOMPSON AND RANKING MEMBER ROGERS: Over the past decade, the Department of Homeland Security (DHS) has been evaluating and testing approaches to determine the most effective manner to add biometrics to its arrival and departure procedures to provide better security while maintaining privacy and facilitating the travel experience. We support those efforts.

The work is being done so that the U.S. Customs and Border Protection (CBP) can implement the congressional mandate to administer a biometric air entry/exit program for departing international air passengers. The Transportation Security Administration (TSA) also is evaluating biometrics for identity verification at the security checkpoint. The primary benefits of the biometric programs are the enhanced ability to protect against identification fraud and to improve DHS's ability to determine the rate of visa overstays.

A4A members have worked closely with CBP and TSA during this process and participated in the DHS Science and Technology Directorate's technology evaluations and pilot programs. DHS has worked to address and meet our principal goals of ensuring that any biometric program would increase security, improve the passenger experience and not require airlines to perform government functions.

The security benefits of biometrics are undeniable. For example, the CBP match rate associated with facial recognition technology is consistently high, above 98 percent, and it is expected that technology will continue to improve. TSA, through collaboration with CBP, also is seeing the benefits of biometric technology, in particular facial recognition technology.

While we believe the privacy protections currently in place are effective, we will continue to work with the DHS, CBP, TSA and our passengers to ensure the highest levels of privacy. Airlines already collect and transmit biographic data to DHS to comply with Federal security requirements, so we have experience in the area. Airlines, like DHS, also have committed to strict privacy principles as it relates to the use of biometric information. For facial recognition technology, these principles include opt-out options and non-retention of photos for business purposes. In fact, airlines and airports must immediately purge images following transmittal to CBP for identity verification. We all agree that privacy is of the utmost importance.

We appreciate the collaboration that DHS has demonstrated in implementing the statutory mandate to administer biometrics to improve our nation's security. We recognize this is an area of rapidly changing technology and public acceptance and we look forward to working with Congress and the Administration to continue to make our nation's aviation system even more secure while improving the passenger experience. We believe that Congress can play a constructive role in incentivizing the best biometrics technology and we look forward to working with you as the technological capabilities continue to advance.

Sincerely,

SHARON PINKERTON
Senior Vice President, Legislative & Regulatory Policy, Airlines for America.

LETTER FROM DOUGLAS E. LAVIN TO CHAIRMAN BENNIE THOMPSON AND RANKING MEMBER MIKE ROGERS

July 8, 2019.

The Honorable BENNIE THOMPSON,
Chairman, Committee on Homeland Security, U.S. House of Representatives, Washington, DC 20515.

The Honorable MIKE ROGERS,
Ranking Member, Committee on Homeland Security, U.S. House of Representatives, Washington, DC 20515.

DEAR CHAIRMAN THOMPSON AND RANKING MEMBER ROGERS: On behalf of the International Air Transport Association (IATA) and its 290 member airlines, I appreciate the opportunity to comment on the use of biometric technologies in aviation. IATA is a strong supporter of the use of biometrics to facilitate a safe, secure, and efficient commercial air travel experience for our members' passengers.

IATA estimates that the number of airline passengers globally will double by 2037. Given that aviation infrastructure development (e.g. airports and air traffic management) will likely not be able to keep pace with such growth, IATA has undertaken several initiatives designed to improve the experience and efficiency of the current travel process, particularly passenger facilitation at airports. IATA's "One ID" program seeks to introduce a streamlined, friction-free, and passenger-centric process that allows an individual to assert their identity to the required level at every process step while maintaining the privacy of personal data. One ID is premised on a single token biometric that can be used at each touchpoint across the end-to-end journey.

In June 2019, the IATA Annual General Meeting passed the attached resolution on the One ID program which affirms the significant benefits of paperless travel by means of biometric recognition and encourages governments to collaborate on a biometric-based identify management solution.

IATA and several our member airlines have also worked closely with U.S. Customs and Border Protection (CBP) on their proposed biometric entry/exit system. We are very pleased with CBP's engagement with industry on this program and their consideration of important operational issues and the protection of passenger privacy. We look forward to continuing to work with CBP in a collaborative fashion as they implement this system.

Thank you for your consideration.

Sincerely,

DOUGLAS E. LAVIN,
Vice President, Member and External Relations—North America.

ATTACHMENT.—RESOLUTION ON ONE ID

RECALLING that global air passenger traffic is projected to double by 2037, meaning that the air transport sector will accommodate an additional four billion passengers by this time;

FURTHER RECALLING that the practical obligation to obtain and check passenger identity documentation and travel authorizations is often placed upon carriers as a part of immigration and border security processes;

ACKNOWLEDGING that a safe, secure and seamless passenger experience is an objective of primary importance for consumers, governments and the airline industry;

RECOGNIZING that efficient and optimized communication standards support both enhanced customer experiences and more effective security outcomes;

FURTHER RECOGNIZING that important shifts in consumer behaviour, together with changing expectations in respect of real-time information, paperless processes and data privacy, require a high degree of collaboration between air transport sector stakeholders;

The 75th IATA Annual General Meeting:

1. AFFIRMS the significant benefits of paperless passenger travel by means of biometric recognition;

2. ENCOURAGES government authorities, member airlines and airports to support the One ID strategy;

3. ENCOURAGES ICAO and its member states to urgently identify specifications for a digital travel credential that will offer a secure and efficient alternative to passports;

4. ENCOURAGES member airlines and all other actors in the air transport system to work together toward a "use case" for such a globally accepted digital travel credential;

5. CALLS on government authorities, member airlines and airports to urgently:

(i) collaborate on identity management solutions for the sharing of identity information to avoid duplication in passenger checks and enable secure paperless processes, with such solutions to satisfy the highest security principles and meet the important requirements of privacy law;

(ii) work together to find interoperable and innovative solutions;

(iii) further explore and apply the benefits of biometric recognition, including in terms of security and speed;

6. ENCOURAGES governments to explore the possibility of offering the verification of passenger identity information as a service.

LETTER FROM SHANE C. DOWNEY TO RANKING MEMBER MIKE ROGERS

July 9, 2019.

Ranking Member Mike Rogers,
House Homeland Security Committee, H2–117 Ford House Office Building, Washington, DC 20515.

DEAR RANKING MEMBER ROGERS: The Global Business Travel Association ("GBTA") is the world's premier business travel and meetings trade organization headquartered in the Washington, DC area with 40 State chapters in the U.S. and operations on six continents. GBTA's 9,000-plus members manage more than $345 billion of global business travel and meetings expenditures annually. GBTA delivers world-class education, events, research, advocacy, and media to a growing global network of more than 28,000 travel professionals and 125,000 active contacts.

GBTA members work for the majority of Fortune 100 companies, buying, sourcing and managing the corporation's travel budget, among other responsibilities like ensuring the safety and security of their travelers. In a well-managed travel program, a corporation can see a return on investment of $20 for every $1 spent.

Air travel is a major part of business travel and corporate spend. GBTA research on the U.S. economic impact of business travel shows 515 million domestic business trips are taken in a year. Nearly 30 percent involve air travel meaning business travelers take to the skies on over 144 million trips a year.

Because of this mass of travelers, GBTA has made secure and efficient travel a key platform of GBTA's legislative policy. GBTA has consistently called for increased security at airports, including the hiring of additional officers to man these critical areas. However, as travel in general, and business travel specifically, has continued to grow exponentially, it has become clear that simply hiring more people is not enough, and that technology and pre-screening of passengers are necessary to support a system that is safe and efficient.

GBTA has been a supporter of U.S. Customs and Border Protection's (CBP) Global Entry and Transportation Security Administration's (TSA) PreCheck since their inception. GBTA believes the use of biometrics and facial recognition is the logical next step to further increase traveler safety and efficiency in moving through security checkpoints.

This support stems from understanding the issues that impact business travel. GBTA surveys of business travelers consistently cite moving through airport security as one of the largest pain points. PreCheck and Global Entry have delivered business travelers a risk-based, intelligence-driven aviation security system that is safe, fast and efficient. Time is money for business travelers, and inefficient procedures reduce business travel due to the "hassle factor" and hurt the economy.

To further illustrate the impact efficient screening can have, look to GBTA's "Business Traveler Sentiment Index," which profiles business travelers' attitudes around business travel and how that impacts their actual travel behavior. Our research shows TSA PreCheck enrollees are significantly more satisfied with air travel than those not enrolled. Two-thirds (66 percent) of travelers enrolled in TSA PreCheck are satisfied with getting through airport security, compared with just 47 percent of business travelers not enrolled in the program. More striking is the impact the program has on the overall travel experience, 66 percent report satisfaction, compared to 54 percent for those not enrolled.

Today's airport experience involves heavy friction and endless queuing at the counter check-in, bag drop, security screening and boarding. As facial recognition security programs expand, meeting the goal of frictionless travel improves. GBTA supports industry, governments and travelers working together to create a multi-layered approach that includes facial recognition for travel security screening purposes. GBTA believes the business traveling public will continue to embrace this security tool provided the following continue to progress:

Data security is paramount, and the operators must ensure all protocols and procedures are followed to ensure the safety of the individual's data;

False Identification Mitigation must continue to advance and be a part of all future plans. Prior to the enactment of Secure Flight, business travelers all too often had their identities confused with others on flight watch lists, causing delays and unnecessary hassles at the airport. Without a mitigation strategy in place, the same could occur with biometrics and facial recognition;

And, travelers are made aware of the ability to opt in and out of facial screening checkpoints.

GBTA encourages Congress to continue to work with the Department of Homeland Security and other key agencies, the security industry and travelers to strengthen and streamline travelers' safety and security.

Sincerely,

SHANE C. DOWNEY,
Vice President, Government Relations, Global Business Travel Association.

Mrs. LESKO. Thank you.

All my questions, Mr. Chairman and Members, are for Mr. Gould.

My first question, Mr. Gould, is the pilot program that you have working with Delta down in Atlanta, where do you get the photos from? Is it opt-in? Do you share—get the database of passports from CBP?

That is my first question.

Mr. GOULD. Yes, ma'am. We use CBP's TVS matching service for that. CBP has access to State Department photos for the back-end matching.

Then it is an opt-in program. Passengers have the opportunity to choose whether to present biometric identification using the facial capture or to present a credential. We see very high rate of people choosing to provide the facial image.

Mrs. LESKO. OK. So just so that I understand, where do you ask them if they want their photo taken?

Mr. GOULD. Ma'am, there are signs throughout the checkpoint area that say we are piloting this technology and that should you choose not to participate, please let the TSO, the officer, know.

As you approach the TDC, the travel document checker position, there is an officer there. The officer will say, you know, do you choose to provide biometric identification? In which case, if the passenger says yes, they are directed to stand in a specific location for that facial capture. So there is interaction with the officer at that point.

Mrs. LESKO. Thank you. That is very informative.

My next question is due to, I guess, the success of CBP's use of biometrics. I think this is—you know, this technology is going to happen. I do agree with other Members that we need to make sure that we have privacy and security in it, of course.

But are you going to use any of the—is TSA planning on looking at how they can work, I guess, with CBP on their success in order to implement it in more airports?

Mr. GOULD. Yes, absolutely, ma'am. That is the reason we are doing the pilot in Atlanta, is to understand that interaction between us and the CBP TVS system and what benefit that system brings to the TSA checkpoint and the identification verification process.

Mrs. LESKO. Good. I am glad that you are working on it, and hopefully we can get a fairly fast turnaround. I probably would be interested in going and seeing what you are doing down in Atlanta myself.

Mr. GOULD. Yes, ma'am.

Mrs. LESKO. Also, Mr. Gould, are you planning on using this, or have you thought of using biometric technology, or do you, for the employees, the airport employees?

Mr. GOULD. Yes, ma'am. We are considering using biometric identification processes for employees as well.

Mrs. LESKO. Thank you.

The reason that I ask that is because from some of our briefings, hearings, I think we have been concerned about insider-type threats. I think what happened up in—what was it, Washington airport? I can't remember where—an employee take a plane and flew it——

Mr. GOULD. Yes, ma'am, Seattle.

Ms. LESKO. Yes, Seattle, Washington. So—and with baggage handlers and those types of things. So it seems to me that it would be logical that we use biometric screening for the employees themselves.

Mr. GOULD. Yes, ma'am. That is certainly something we will be looking at.

Mrs. LESKO. Thank you.

I yield back my time.

Mr. PAYNE [presiding]. Thank you. We now recognize the gentlelady from Texas for 5 minutes of questioning.

Ms. JACKSON LEE. Mr. Chairman, thank you very much.

I want to start off by asking unanimous consent to put into the record an op-ed by the *Houston Chronicle,* Real Abuses at the Border: Squalid conditions for detained migrants are worthy of all outrage Americans can muster. Ask unanimous consent.

Mr. PAYNE. Without objection.

[The information follows:]

BORDER PATROL ABUSES REAL, AND WORTHY OF OUTRAGE

The Editorial Board, July 5, 2019, Updated: July 5, 2019 8:59 a.m., Houston Chronicle

A ticking time bomb.

That's how a senior manager described the situation at a Border Patrol detention facility in the Rio Grande Valley, according to a report by the Office of Inspector General released this week. The independent watchdog's findings describe squalid, overcrowded conditions at several facilities, where men, women and children are poorly fed and held without access to showers, sometimes for weeks.

The investigators' words and images—men crammed together in standing-room-only cells, dozens of women and children lying side to side on concrete floors—support the testimony of doctors and lawyers who spoke out last week after interviewing immigrants in detention. They also lend credence to the stories Democratic lawmakers heard during a recent visit to a holding facility outside El Paso.

Some had dismissed these claims as politically self-serving, or as the embellishments of partisans and activists looking to gin up outrage. Turns out the government's own reporting shows conditions at these detention centers are worthy of all the outrage Americans can muster.

Along with overcrowding, investigators found more than 800 of the 2,669 children in custody at the facilities had been held longer than 72 hours, violating a court settlement as well as Customs and Border Protection policy. This included a group of 50 unaccompanied children under 7 years old, some of whom had been in these deplorable circumstances for more than 2 weeks.

This report follows a similar warning by the OIG in May after a visit by investigators to holding locations in the El Paso area.

The excuse that the government has been overwhelmed by the number of arrivals, many asylum-seekers from Central America, has worn thin. During a previous increase under the Obama Administration in 2014, mostly by unaccompanied minors, officials were also unprepared. Yet they quickly opened detention space across the country while officials made arrangements for the children to be released as quickly as possible into the custody of family or other sponsors. Although it was far from an ideal situation—this is where the first images of "children in cages" came from—it relieved overcrowding and sped up processing time.

The numbers this time around are larger, but the response has been anemic—seemingly, by design.

So far, the lack of urgency in easing these conditions fits squarely into the spirit of deterrence through pain that has been at the heart of U.S. immigration policies over the years, but which have hardened unconscionably during the Trump administration.

The need to quickly move detained immigrants from Border Patrol custody intensified on Monday, after some of the exchanges of a private Facebook group were released. As reported by ProPublica, group members, including current and former Border Patrol agents, posted racist, sexist and violent memes about immigrants and New York Congresswoman Alexandria Ocasio-Cortez.

On an image of a migrant fording the Rio Grande while dragging a young boy in a plastic bag, group members wrote disparaging comments such as, "At least it's already in a trash bag." Under a photo of a father and his 23-month-old daughter who drowned in the river, the member who posted the image asked if it was fake because the "floaters" were so "clean."

The revelation of the Facebook group comes on the heels of text messages between Border Patrol agents made public as part of an ongoing court case in Arizona, where an agent is accused of knocking down a Guatemalan man with his vehicle and then covering it up. In one exchange, the agent refers to immigrants as "disgusting subhuman s--- unworthy of being kindling for a fire."

All these statements are vile and intolerable, but this isn't just name calling. When these attitudes are brought to bear, they can mean the difference between life and death. Between ignoring the jugs of water that humanitarian groups leave for migrants in the desert or slashing and stomping them. Between taking cover with your fellow agents as rocks fly overhead from across the border fence or indiscriminately shooting into Mexico at anything that moves.

Of course, that side of Border Patrol is countered with the many agents who act humanely while fulfilling their duties, who put their lives on the line to protect immigrants and enforce our laws. But even some of the good actors are pressured to remain silent by a culture that protects its own, no matter the cost, while whistleblowers are ostracized.

Tolerance of these attitudes has gone on long enough.

The House Judiciary and Oversight Committees announced hearings next week into the conditions at detention centers. That's a good start. The agents who violated policy, and basic human decency, should also be punished. And over time, leadership should not only set an example, but work to improve the culture at the Border Patrol, which for far too long has gotten away with little accountability or transparency.

Meanwhile, the time bomb keeps ticking.

Ms. JACKSON LEE. Ask unanimous consent from the *CNET* article, Monday, July 9, Acting DHS Secretary Defends Border Conditions.

Mr. PAYNE. Without objection.

[The information follows:]

DHS OFFICIAL DEFENDS CONDITIONS AT BORDER PATROL STATIONS

July 8, 2019.

WASHINGTON (AP).—Acting Homeland Security Secretary Kevin McAleenan on Sunday defended conditions at U.S. Border Patrol stations following reports of crowded and unsanitary conditions that have heightened debate about President Donald Trump's immigration policy, a trademark issue for his reelection campaign.

"It's an extraordinarily challenging situation," McAleenan told ABC's "This Week."

The Homeland Security Department's internal watchdog provided new details Tuesday about the overcrowding in Texas' Rio Grande Valley, the busiest corridor for illegal crossings. The report said children at three facilities had no access to showers and that some children under age 7 had been held in jammed centers for more than 2 weeks. Some cells were so cramped that adults were forced to stand for days on end.

Government inspectors described an increasingly dangerous situation, both for migrants and agents—a "ticking time bomb," in the words of one facility manager. The report echoed findings in May by the department's inspector general about holding centers in El Paso, Texas: 900 people crammed into a cell with a maximum capacity of 125; detainees standing on toilets to have room to breathe; others wearing soiled clothing for days or weeks.

In tweets Sunday afternoon, Trump went further than McAleenan in defending his administration's response, accusing the news media of "phony and exaggerated accounts" but without providing evidence.

"Border Patrol, and others in Law Enforcement, have been doing a great job. We said there was a Crisis—the Fake News & the Dems said it was 'manufactured,'" Trump wrote. Federal detention centers "are crowded (which we . . . brought up, not them) because the Dems won't change the Loopholes and Asylum. Big Media Con Job!"

Democrats faulted Trump for not offering an immigration overhaul that could pass a divided Congress.

"The president is acting like we are some weak, pathetic country," said Colorado Sen. Michael Bennet, a Democratic Presidential candidate. "We have the ability to treat human beings humanely. We have the ability to lead our hemisphere in a discussion about how to deal with this refugee crisis," he said on "Fox News Sunday."

McAleenan said that since the first of the year, 200 medical providers have been added to facilities, including personnel from the U.S. Coast Guard and the Public Health Service Commission Corps.

"We have pediatricians in border patrol stations for the first time in history trying to help address conditions where children are coming across 300 a day in . . . April and May," McAleenan said.

"We've built soft-sided temporary facilities. These are spaces that are much more appropriate—high ceilings, more room for children and families. We've put them both in Donna, Texas, in South Texas as well as in El Paso to provide additional space . . . We've bought buses to transport people to better places."

McAleenan disputed news reports, including those by The Associated Press, of especially troubling conditions at a border station in Clint, Texas, where a stench was coming from children's clothing and some detainees were suffering from scabies and chickenpox.

"There's adequate food and water," he said. "The facility's cleaned every day, because I know what our standards are and I know they're been followed because we have tremendous levels of oversight. Five levels of oversight.

"Inadequate food, inadequate water and unclean cells. None of those have been substantiated."

He said everyone in the chain of command is worried about the situation of children detained at the border. He said that on June 1, his department had 2,500 children in custody, including 1,200 who had been there for more than 3 days. As of Saturday, McAleenan said there were 350 children, and only 20 have been in the department's custody for more than 3 days.

"So that's huge improvement based on the resources we asked for from Congress and were finally given," he said.

Sen. Jeff Merkley, D-Ore., told NBC's "Meet the Press" that he is stunned when administration officials say that reports on the conditions are unsubstantiated.

"I'm just like, 'What world are they living in?'" Merkley said, citing government and news reports. "From every direction you see that the children are being treated in a horrific manner. And there's an underlying philosophy that it's OK to treat refugees in this fashion. And that's really the rot at the core of the administration's policy."

Separately, McAleenan addressed questions about U.S. Border Patrol agents who are under fire for posting offensive messages in a "secret" Facebook group that included sexually explicit posts about U.S. Rep. Alexandria Ocasio-Cortez and dismissive references to the deaths of migrants in U.S. custody. The existence of that group was reported Monday by ProPublica. Prior to that, few people outside the group had ever heard of it.

He said an allegation about such activity was investigated in 2016. "Discipline was meted out on an agent that made an offensive post on that website," he said.

Ms. JACKSON LEE. I ask unanimous consent to put into the record the IG inspector's report, dated July 2, 2019.

Mr. PAYNE. Without objection.*

Ms. JACKSON LEE. I ask to put into the record an article found in *The New York Times*, ICE uses facial recognition to mine State driver's license. That is July 7. Ask unanimous consent.

Mr. PAYNE. Without objection.

[The information follows:]

ICE USED FACIAL RECOGNITION TO MINE STATE DRIVER'S LICENSE DATABASES

By Catie Edmondson, July 7, 2019.

WASHINGTON.—Immigration and Customs Enforcement officials have mined state driver's license databases using facial recognition technology, analyzing millions of motorists' photos without their knowledge.

In at least three 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 two 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.

The documents, obtained through public records requests by Georgetown Law's Center on Privacy and Technology and first reported on by The Washington Post, mark the first known instance of ICE using facial recognition technology to scan state driver's license databases, including photos of legal residents and citizens.

Privacy experts like Harrison Rudolph, an associate at the center, which released the documents to The New York Times, said the records painted a new picture of a practice that should be shut down.

"This is a scandal," Mr. Rudolph said. "States have never passed laws authorizing ICE to dive into driver's license databases using facial recognition to look for folks."

He continued: "These states have never told undocumented people that when they apply for a driver's license they are also turning over their face to ICE. That is a huge bait and switch."

The use of facial recognition technology by law enforcement is far from new or rare. Over two dozen states allow law enforcement officials to request such searches

*The information has been retained in committee files and is available at *https://www.oig.dhs.gov/sites/default/files/assets/2019-07/OIG-19-51-Jul19__.pdf*.

against their databases of driver's licenses, a practice that has drawn criticism from lawmakers and advocates who say that running facial recognition searches against millions of photos of unwitting, law-abiding citizens is a major privacy violation.

The F.B.I., for example, has tapped state law enforcement's troves of photos—primarily those for driver's licenses and visa applications—for nearly a decade, according to a Government Accountability Office report. The bureau has run over 390,000 searches through databases that collectively hold over 640 million photos, F.B.I. officials said.

The Georgetown researchers' documents covered 2014 to 2017, and it was not immediately clear if those states still comply with the ICE requests. Representatives for the states' motor vehicles departments could not immediately be reached for comment Sunday night.

On Monday, Amy Tatko, the public outreach manager for the Vermont Agency of Transportation, said in a statement that the use of facial recognition technology by the agency was discontinued in 2017 "at the direction of current Governor Phil Scott as soon as it was brought to his attention."

Matt Bourke, an ICE spokesman, said the agency would not comment on "investigative techniques, tactics or tools" because of "law-enforcement sensitivities."

But he added: "During the course of an investigation, ICE has the ability to collaborate with external local, Federal and international agencies to obtain information that may assist in case completion and subsequent prosecution. This is an established procedure that is consistent with other law enforcement agencies."

The researchers sent public records requests to each state, searching for documents related to law enforcement's relationship with state motor vehicles departments. They received varying degrees of responsiveness but discovered the ICE requests in Utah, Washington and Vermont, which have come under fire before for sharing driver's license information with the agency.

The Seattle Times reported last year that Washington State's Department of Licensing turned over undocumented immigrants' driver's license applications to ICE officials, a practice its Governor, Jay Inslee, pledged to stop. And a lawsuit in Vermont filed by an activist group cited documents obtained under public records law that showed that the State Department of Motor Vehicles forwarded names, photos, car registrations and other information on migrant workers to ICE, Vermont Public Radio reported this year.

The relationship between Washington's Department of Licensing and ICE officials may prove to be particularly interesting to privacy experts because of a law the State Legislature passed in 2012 stipulating that the department could use a facial recognition matching system for driver's licenses only when authorized by a court order, something ICE did not provide.

Facial recognition technology has faced criticism from experts who point to studies that show that recognition algorithms are more likely to misidentify people of color—and in particular, women of color. At least 25 prominent artificial-intelligence researchers, including experts at Google, Facebook and Microsoft, signed a letter in April calling on Amazon to stop selling its facial recognition technology to law enforcement agencies because it is biased against women and racial minorities.

The use of the technology has also come under fire from a bipartisan group of lawmakers. The House Homeland Security Committee, led by Representative Bennie G. Thompson, Democrat of Mississippi, will hold a hearing on Wednesday grilling Department of Homeland Security officials about their use of facial recognition. The chairman of the House Committee on Oversight and Reform, Representative Elijah E. Cummings of Maryland, has pledged to investigate the use of the rapidly expanding technology in the public and private sectors.

"This technology is evolving extremely rapidly, without any, really, safeguards, whether we are talking about commercial use or government use," Mr. Cummings said at a hearing on the issue last month. "There are real concerns about the risks that this technology poses to our civil rights and liberties, and our right to privacy."

Ms. JACKSON LEE. First of all, let me say to all of you, let me thank you for your service to the Nation. I have had the privilege of serving on this committee for a very, very long time.

Mr. Wagner, I will get to the underlying basis of this hearing. But let me be very clear that I have to speak with great ire and dismay for the behavior of individuals at the border and the refusal of the Department of Homeland Security to cooperate with Members of Congress.

I want to indicate that the $4.6 billion that was given last week and the whining that went on for a period of time to blame Congress was a misrepresentation to the American people.

Because we understand that reprogramming of dollars can happen at the drop of a hat. The reason why I say that is, as I go into my questioning regarding the facial recognition, unless the answer changed from the time I was here, I understand there is no statutory legislation or anything that is giving you that authority. You are going to look for it. Maybe you will answer that question differently.

But I just quickly want to say that we will not be able to tolerate—we respect you as servants of the Nation. It is unfortunate that very destructive policies of this administration has tainted very fine American servants of the people. That is what happened. Because when you don't have toothpaste and a toothbrush and you have a truckload of that material or nonprofits like the conscious presence that I met at the border station, one, and also Clint, begging to be of help, and you are telling the American people there is no one helping you, I think it is a sad commentary.

So I just want to make sure you are aware of my dismay, that will not be tolerated, and the mismanagement will not be tolerated, and the accusations against Members will not be tolerated.

If Vice President Pence can go in and look after it is cleaned up, spic and span, then Members who have oversight responsibility should be able to go in and look.

Mr. WAGNER. Understood.

Ms. JACKSON LEE. I would appreciate it if you would report that back to the Secretary.

Mr. WAGNER. I will.

Ms. JACKSON LEE. Thank you. Let me say to the gentleman from Transportation Security Administration, I am interested in you looking into the treatment of Crystal Lynette Sonea and Sharif Mohamad Hotef—we will give you that information—around April 14 in the Atlanta airport.

So let me start with Mr. Wagner. This is horrific, the information regarding the use of these—and my earlier information was that you know that people of color and women—so I get it twice—are unfortunately targeted the most.

In the article, it says agents with the FBI and ICE have turned the State driver's license databases recognition into a gold mine scanning through hundreds of millions of American photos without their knowledge or consent.

In addition, it says that the State department motor vehicle databases into the bedrock of unprecedented surveillance and infrastructure.

I want to submit into the record, Mr. Chairman, an article by Amazon that says "Amazon facial recognition"—not by Amazon—"Amazon facial recognition mistakenly confused 28 Congresspersons with known criminals". I will not put the Congressperson's names into the record, but I think most of us would like not to be known as known criminals.

My question——

Mr. PAYNE. No objection.

[The information follows:]

AMAZON'S FACIAL RECOGNITION WRONGLY IDENTIFIES 28 LAWMAKERS, A.C.L.U. SAYS

By Natasha Singer, July 26, 2018, New York Times.

Representative John Lewis of Georgia and Representative Bobby L. Rush of Illinois are both Democrats, members of the Congressional Black Caucus and civil rights leaders.

But facial recognition technology made by Amazon, which is being used by some police departments and other organizations, incorrectly matched the lawmakers with people who had been charged with a crime, the American Civil Liberties Union reported on Thursday morning.

The errors emerged as part of a larger test in which the civil liberties group used Amazon's facial software to compare the photos of all Federal lawmakers against a database of 25,000 publicly available mug shots. In the test, the Amazon technology incorrectly matched 28 Members of Congress with people who had been arrested, amounting to a 5 percent error rate among legislators.

The test disproportionally misidentified African-American and Latino Members of Congress as the people in mug shots.

"This test confirms that facial recognition is flawed, biased and dangerous," said Jacob Snow, a technology and civil liberties lawyer with the A.C.L.U. of Northern California.

On Thursday afternoon, three of the misidentified legislators—Senator Edward J. Markey of Massachusetts, Representative Luis V. Gutiérrez of Illinois and Representative Mark DeSaulnier of California, all Democrats—followed up with a letter to Jeff Bezos, the chief executive of Amazon, saying there are "serious questions regarding whether Amazon should be selling its technology to law enforcement at this time."

In the letter, the lawmakers asked for details on how Amazon tested its facial technology for accuracy and bias. They also requested a list of all government agencies using Amazon's facial technology as well as all law enforcement and intelligence agencies Amazon had communicated with about the system.

Separately, two other congressmen wrongly matched with mug shots—Mr. Lewis and Representative Jimmy Gomez, a California Democrat—wrote their own letter to Mr. Bezos requesting an immediate meeting "to discuss how to address the defects of this technology." The letter was first obtained by BuzzFeed.

Nina Lindsey, an Amazon Web Services spokeswoman, said in a statement that the company's customers had used its facial recognition technology for various beneficial purposes, including preventing human trafficking and reuniting missing children with their families. She added that the A.C.L.U. had used the company's face-matching technology, called Amazon Rekognition, differently during its test than the company recommended for law enforcement customers.

For one thing, she said, police departments do not typically use the software to make fully autonomous decisions about people's identities. "It is worth noting that in real-world scenarios, Amazon Rekognition is almost exclusively used to help narrow the field and allow humans to expeditiously review and consider options using their judgment," Ms. Lindsey said in the statement.

She also noted that the A.C.L.U had used the system's default setting for matches, called a "confidence threshold," of 80 percent. That means the group counted any face matches the system proposed that had a similarity score of 80 percent or more. Amazon itself uses the same percentage in one facial recognition example on its site describing matching an employee's face with a work ID badge. But Ms. Lindsey said Amazon recommended that police departments use a much higher similarity score—95 percent—to reduce the likelihood of erroneous matches.

Facial recognition—a technology that can be used to identify unknown people in photos or videos without their knowledge or permission—is fast becoming a top target for civil liberties groups and privacy experts.

Proponents see it as a useful tool that can help identify criminals. It was recently used to identify the man charged in the deadly shooting at The Capital Gazette's newsroom in Annapolis, Md.

But civil liberties groups view it as a surveillance system that can inhibit people's ability to participate in political protests or go about their lives anonymously. This month, Microsoft said the technology was too risky for tech companies to deploy without government oversight and called on Congress to regulate it.

Over the last 2 months, Amazon has come under increasing pressure for selling its Rekognition technology to law enforcement agencies. The company has sold the service as a way for police departments to easily identify suspects in photos or videos.

Amazon's site describes how its system can perform "real-time face recognition across tens of millions of faces" and detect "up to 100 faces in challenging crowded

photos." (The New York Times recently used the Amazon technology to help identify guests at the royal wedding of Prince Harry and Meghan Markle.)

In May, two dozen civil liberties groups, led by the A.C.L.U., wrote a letter to Mr. Bezos, demanding that his company stop selling the facial technology to law enforcement. The groups warned that the software could be used to trail protesters, undocumented immigrants or other members of the public—not just criminal suspects.

Similar demands of Mr. Bezos from Amazon employees, Amazon investors, and several hundred academics soon followed.

Mr. Snow of the A.C.L.U. said his group's test of Amazon's software should push Congress to put a moratorium on law enforcement's use of facial recognition technology.

But in a blog post last month, Matt Wood, general manager of artificial intelligence at Amazon Web Services, said that there had been no reports of law enforcement abuse of Amazon's facial technology. He added that Amazon believed it was "the wrong approach to impose a ban on promising new technologies because they might be used by bad actors for nefarious purposes in the future."

In a letter to Amazon, the Congressional Black Caucus noted the potential for racial bias with the technology—an issue raised by a recent M.I.T. study that found some commercial facial recognition systems correctly identified a higher proportion of white men than darker-skinned women. In their letter, the caucus members urged Mr. Bezos to hire "more lawyers, engineers and data scientists of color to assist in properly calibrating this technology to account for racial bias that can lead to inaccuracies with potentially devastating outcomes."

In the civil liberties group's test, the Amazon software misidentified several members of the Congressional Black Caucus, including Mr. Lewis and Mr. Rush, as other people who had been arrested.

"We think these test results really raise the concern that facial recognition has a race problem," said Mr. Snow, the A.C.L.U. lawyer.

Ms. JACKSON LEE. To both of you, and a little extra time for them to answer, the two gentlemen from TSA and from CBP, how are you doing this, with the protections of due process and notice, without the notice of the American people that the process even exists? What framework is there to have the firewalls that you are not turning Congress people or children into convicted criminals?

Mr. WAGNER. We are not seeing those same error rates that are—that can be attributed to specific demographics in how we are doing this.

How we are doing this cannot be compared to previous studies on this. There are different control factors in place. You know, there are different—we are taking a person that is standing in front of a camera where we can take a clear picture, and we are comparing it against a clear set of baseline photos from their passports or their visas where they were also standing still in front of a camera to capture a clear picture. That is why we have such accurate rates.

Previous studies didn't quite take the same control factors into place. This is not us taking an image of a person and randomly running it against a gallery set of indistinguishable, say, quality photographs and lowering down the accuracy rate as to what constitutes a match to make it match someone that it is not.

I mean, you can do the same thing with fingerprints. If you only take two——

Ms. JACKSON LEE. How do you secure that—how do you secure that data?

Mr. WAGNER. When the photo is taken at the airport, it is encrypted and transmitted to the CBP into our cloud space. It is then templatized, which my understanding of that is it is turned into a mathematical formula. There is a unique identifier associated with that. There is no biographical data or PII associated with

that. It is matched up against our gallery of templatized photos. When there is a match, a message goes back to the camera with just yes or no and that unique identifier.

Ms. JACKSON LEE. Let me move quickly to Mr. Gould and TSA. Let me thank TSA for their front-line service of protecting America.

Mr. PAYNE. Thank you, Ms. Lee.

Ms. JACKSON LEE. Thank you, Mr. Chairman, for your indulgence.

The same question as to how you are utilizing and how you are protecting the data and avoiding this intrusion into the privacy of the American public without them knowing it.

Mr. GOULD. Yes, ma'am. So I would—we are using CBP's TVS system. So the answer that Mr. Wagner provided applies to TSA as well.

With respect to the accuracy and the matching, the one thing that I would like to add is, the technology is evolving so quickly and it is improving so quickly, we will continue to assess at every step, for any additional pilots, from when we consider employing this in a wider scale, we will assess the best way to get quality image capture and be sure to employ the highest-quality algorithms to ensure the highest match rate.

Mr. PAYNE. OK. Thank you.

Ms. JACKSON LEE. Thank you, Mr. Chairman.

I yield back. Thank you very much.

Mr. PAYNE. The Chair recognizes Mr. Green.

Mr. GREEN of Texas. Thank you, Mr. Chairman.

Thank the Ranking Member. Thank the witnesses for appearing.

My questions have to do with the surveillance. My first question is, are all people who are traversing areas within an airport under some degree of suspicion?

Who would like to answer, please?

Mr. GOULD. Well, I would say that when a person is traversing an airport, they are not necessarily under suspicion. Airports, you know, utilize security cameras, closed circuit television, for security reasons.

With respect to TSA, though, the only reason that we use cameras and capture images is solely for the purpose of identification.

Mr. WAGNER. If I could just add that——

Mr. GREEN of Texas. Please.

Mr. WAGNER [continuing]. What we are doing is absolutely not a surveillance program. The picture of an individual is taken with their complete knowledge, because they are standing in front of a camera at a time and place where they have to present a physical ID in order to establish their identity to move forward. We are just replacing the evaluation and the scrutiny of the physical ID with a computer algorithm.

Mr. GREEN of Texas. Should I assume that persons who enter the airport and who are not within the secured area will not be a subject of this technology?

Mr. GOULD. Not by TSA, sir. It solely occurs at either the bag drop or the checkpoint.

Mr. WAGNER. Or a time and place where you have to present an identification to establish your identity to go through whatever process that is.

Mr. GREEN of Texas. In Houston, the bag drop occurs outside of the building, before you enter the building. You drive up in your car, you have friends, neighbors with you perhaps, and you go over to an agent, and that person then receives your bag, gives you a ticket.

So would it occur in this area, please?

Mr. GOULD. Sir, right now, the only place that the biometric identification that the bag drop is occurring is in Terminal F in Atlanta. I went down there. I observed the way the technology——

Mr. GREEN of Texas. If I may, because time is of the essence. But we are talking about expanding, are we not?

Mr. GOULD. Yes, sir.

Mr. GREEN of Texas. OK. Here is my concern. Let me go to the point, and I will be as pithy as I can.

But one can only imagine what Mr. J. Edgar Hoover would have done with this technology. It was Mr. Hoover who surveilled Dr. King. They went so far as to send a letter to Dr. King encouraging him to take his life. One can only imagine.

Now, I am not placing you under the eye of suspicion, but it is my job to make sure that this kind of technology is not abused. I take my job seriously because I am protecting you by doing my job.

So my concerns are, do you alert people in some way to—so as to advise them that they are being surveilled?

Mr. GOULD. Sir, I wouldn't characterize it as surveillance. The way the alert happens, to use your term, is when you approach the bag drop, the agent will say, "Would you like to use biometric identification to match you to your bag?" or something along those lines.

Mr. GREEN of Texas. Permit me to ask this. If you thought—if you believed that this was a form of surveillance, would you alert people? Would you alert the public, if you thought this was some form of surveillance?

Mr. GOULD. So we don't do surveillance, but we are——

Mr. GREEN of Texas. Excuse me. If you thought—would you recommend—if we were of the opinion that this is surveillance, what do you think we should do? Should we indicate that person should be noticed that they are being surveilled?

Mr. GOULD. Sir, we provide notice before the image is captured. It is purely with the consent of the traveler.

Mr. GREEN of Texas. What about the consent of the person who happens to be with the traveler who is just a friend?

Mr. GOULD. We solely capture the picture of the traveler who has consented. The camera is only about 2 feet away. You step right in front of it, and it solely captures that image.

Mr. GREEN of Texas. All right. Thank you. But we are considering expansion.

My concern is suspicionless surveillance, suspicionless surveillance, surveilling persons who are not under suspicion perhaps by accident.

Final question is this because time is running out.

Will there be any means by which persons who engaged in litigation can acquire access to this intelligence that you have preserved for some length of time, meaning the photographs?

Will there be any means by which persons who are engaged in litigation can acquire it?

Mr. GOULD. Sir, the photographs we match against are in the CBP TVS system. They are passport photographs. The images that are captured are not retained in the camera in any respect. We solely get back a match/no match return, if that answers your question.

Mr. GREEN of Texas. It really does not, because what I am trying to get to is this: If persons are engaged in some form of litigation—and one can only imagine what that might be—will they be able to acquire a photo so as to show that a person was at a given location on a given occasion?

Mr. GOULD. I understand, sir. That photo is not retained at all by TSA, so they will not be maybe to retain it.

Mr. GREEN of Texas. It is retained——

Mr. GOULD. It is encrypted. It is transmitted to CVP, and a match rate is returned.

Mr. GREEN of Texas. OK.

Mr. WAGNER. If it is a U.S. citizen, the photo is deleted after 12 hours. If it is a foreign national, at the baggage drop, that photo would also be deleted. What we would keep on a foreign national, though, is their boarding on the plane and their final departure to serve as the biometric exit of their departure.

Mr. GREEN of Texas. Thank you. I greatly appreciate this. I assure you that I want us to secure our airports, our ports of entry, but I am also concerned about suspicionless surveillance.

Thank you.

Mr. PAYNE. Thank you.

The gentleman, Mr. Guest, you are recognized for 5 minutes.

Mr. GUEST. Thank you, Mr. Chairman.

Mr. Wagner and other guests, thank you for being here today. I know that at least 3 of our witnesses, your departments fall under the Department of Homeland Security.

Your website reads as follows: The Department of Homeland Security has a vital mission: To secure the Nation for the many threats we face. This requires the dedication of more than 240,000 employees in jobs that range from aviation and border security to emergency response, from cybersecurity analysts to chemical facility inspectors. Our goal is clear: Keeping America safe.

In addition to the agencies that are represented here today, Homeland Security includes the Cybersecurity and Infrastructure Security Agency, the United States Citizen and Immigration Services, the United States Coast Guard, the United States Immigration and Customs Enforcement. It includes FEMA as well as the Customs and Border Protection, Secret Service, and the TSA.

I believe that if these agencies that I just spoke of, if these agencies were abolished, that our country would be substantially less safe.

My question—I will begin with you, Mr. Wagner—is can you please tell me what impact it would have on the people of America if Homeland Security and these agencies for which you serve, if these agencies were abolished by Congress?

Mr. WAGNER. Well, there would be no one to process people coming and going across the border, either U.S. citizens or visitors.

There would be no one to process commercial cargo, to look for harmful goods or products coming in. There would be no one to collect the taxes that are due on those duties. CBP collects over $40 billion a year into the U.S. Treasury through duties, taxes, and fees. There would be no one to do that.

Mr. GUEST. Would you agree with me that the different enforcement capacities that the Department of Homeland Security polices, that it runs a gamut of different things? We just talked about everything from the Secret Service, which provides protection for our dignitaries; TSA, which is responsible for air travel; Coast Guard; border enforcement—that those are very important functions of our Government to make sure that these agencies are funded? Would you agree with that, Mr. Wagner?

Mr. WAGNER. Yes. The origins of our agency go back to 1789 and the very beginning of the country.

Mr. GUEST. Mr. Gould, would you care to expound on that at all?

Mr. GOULD. I agree with what Mr. Wagner said, and, you know, if TSA were not there, the security of transportation systems, not solely air travel, would be in some degree of jeopardy.

Mr. DI PIETRO. Congressman, as you indicated, you know, we protect the President and the Vice President, others. We also have criminal investigations. So that is critical work that we are doing.

Mr. GUEST. Would each of you agree that it would be irresponsible to talk about abolishing these agencies that perform such very important tasks on behalf of the American people?

Mr. WAGNER. Yes.

Mr. GOULD. Yes, sir.

Mr. DI PIETRO. I would agree with that.

Mr. GUEST. No further questions, Mr. Chairman. I yield back.

Mr. PAYNE. Thank you. I, you know, just—I know I was late to the hearing today, but I don't really—and maybe it happened before I got here, but I don't really ever mention—hearing anyone mention that these institutions should be abolished, so just for the record.

We have the gentleman from Kansas City, Mr. Cleaver.

Mr. CLEAVER. Thank you, Mr. Chairman.

I am deviating a little. Do you know James Wilson? Do any of you know who he is? Probably one of the most important figures that we don't know much about. He signed the Declaration of Independence and eventually became a member, 1 of the first 6 members of the Supreme Court. He said that the Congress shall form the grand inquisition of the Executive branch. I think that my children's children, and even their children, will study this era and say: That is when it got started.

I am concerned, you know, I was in the executive branch municipality, mayor of Kansas City, and so I know you guys are busy, especially right now. A group of my colleagues and I signed a letter and sent it to you, Mr. Wagner and Mr. Gould, almost 30 days ago. We haven't gotten an answer. So I didn't know if this was a part of the plan to ignore Congress or if you are just consumed. I am not stupid, so I know you don't have—nobody should expect you to write a personal letter to everybody who writes you a letter, even Members of Congress, but if you don't have enough staff, we need to know. Because until it completely collapses, we are still sup-

posed to provide oversight. I am not trying to be hostile. I am not sure I can do a good job of being hostile, but I can certainly do a good job of being frustrated. So I appreciate your work and what you do, but I just—I have to say that it is frustrating, just listening, just seeing what is going on, refusal after refusal to allow Congress to do its oversight. I hope that if I am around at a time when my voice is important, to say, I am not going to support nonresponsiveness to Congress, that I get the opportunity to say it, even if my daddy is in the White House.

Now, having said that, some of the questions that my colleagues and I asked because we thought they were important, I will ask a couple of them. Time is running out, but is there any statutory authority that would allow the whole process of facial recognition, or is that just an internal move? Anybody?

Mr. WAGNER. There are several pieces of statutory authority that authorize us to do and run this program. There are several pieces of legislation from Congress, requiring a biometric-based, entry-exit system for certain foreign nationals. There are other statutes which authorize us to determine identity and citizenship, including U.S. citizens. There has to be a way for us to make that determination that a person is a U.S. citizen, and there are statutes to authorize us to consider evidence presented by that person to make that determination, and then if it is not to the examining officer's satisfaction, the regulations stipulate that person would be considered and inspected as an alien.

Mr. CLEAVER. OK. Thank you.

Mr. Gould.

Mr. GOULD. Sir, from a TSA perspective, the Aviation and Transportation Security Act requires that we screen all passengers and crew boarding aircraft. Fundamental in that screening process is that we positively identify them. The Act mentions exploring the use of biometrics for that purpose. So that is the authority that we are operating under.

Mr. CLEAVER. OK. I mean, it wasn't a trick question. I just wanted to know.

Mr. GOULD. No, I understand, sir.

Mr. CLEAVER. Yes. Last week, I participated in a demonstration in front of the Treasury Department, along with a number of other individuals, the refusal to put a Congressionally-approved likeness of an African American woman on the dollar. That is another whole issue, but I was in front of the demonstration. Should I and the other folk who got off that bus to demonstrate expect that we were somehow surveilled and put in the category of subjects of interest? I mean, since that is what apparently takes place on the grounds of the White House. I don't want to suggest I am as important as, you know, the President or Patrick Mahomes or somebody, but, you know, should I expect that?

Mr. DI PIETRO. Congressman, we do have a CCTV video surveillance system in and around the White House. There is a PIA that is published through the Department of Homeland Security alerting people to that. In addition, the cameras that we have, many of them are overt, all down Pennsylvania Avenue and on the buildings adjacent to the White House there.

Mr. CLEAVER. What about other Federal departments?

Mr. DI PIETRO. I can't speak to what other Federal Departments are doing, Congressman.

Mr. CLEAVER. OK. All right. Thank you.

Mr. Gould, nice suit.

Mr. GOULD. Thank you very much, sir. I like yours, too.

Mr. CLEAVER. I yield back, Mr. Chair.

Mr. PAYNE. Thank you, sir. Now we recognize the gentlelady from Florida, Mrs. Demings.

Mrs. DEMINGS. Thank you so much, Mr. Chairman, and thank you to our witnesses today. Let me just for the record say that I respect the jobs that you have to do. I understand how tough they are. I think that all of our jobs have gotten tougher in recent years. I am not sure why my colleague felt the need to talk about abolishing your agencies, because I know no one on this committee, on either side of the aisle, has ever proposed such an idea. We are the Committee on Homeland Security, and we are here to make sure that you have the tools and resources to effectively do your jobs, but I know that gets a little tougher when sometimes you receive unjust and improper orders and do not have the resources to effectively do your job.

Earlier I heard one of my colleagues talk about the reason for biometric technologies involved speed and efficiency. Well, I was assigned to the Orlando International Airport as a police commander on the worst day in aviation history, on 9/11. I know that the No. 1 responsibility for you is the safety of the traveling public, and if you can ensure that, or increase those odds and do it in an efficient and faster way, then that is just icing on the cake.

But what sets us apart as we work to keep our Nation safe, what sets us apart in this country is that we can enforce the laws and write the laws, but also protect an individual's civil rights. That is what sets us apart. I will not—violating civil rights or the perception of violating civil rights is an issue that we cannot ignore and we have to deal with. Look, when we are able to deploy new technology, that is a great and wonderful thing. I remember how exciting that was, but it is our job, on the committee, and your jobs, as the head of your agencies, to make sure that we can do it all. I believe in this Nation we can.

I know we have talked about every different thing that we possibly could. We do thank you for your endurance. I just want to go back for just a minute to testing for accuracy and any biases. Could you tell me who sets the minimum standards for this particular program, like, who decides what testing is done for accuracy or bias, is conducted before deploying the technology? How do you get that baseline and say that this technology, we have done the testing, we have spoken to the stakeholders, we are ready for prime time now? Understanding, as I believe you said earlier, that we are always fine-tuning and going back and checking up, but who sets the original kind-of standards before deployment? What is acceptable and unacceptable? Mr. Wagner, we will start with you.

Mr. WAGNER. Sure. So we would do that internally. We would determine what constitutes a match versus a nonmatch to a photo. We would evaluate this with our DHS Science and Technology Department. We would do it in consultation with NIST. We do it in consultation with experts from the industry and the vendors of this

equipment. We have partnered with NIST, and starting this summer into the fall, we will be deeply analyzing the results of our data to make sure that we are not seeing those error rates that are attributable to a certain demographic. We are not seeing it from our internal review of it, but we want to make sure, so we are bringing the experts in to make sure——

Mrs. DEMINGS. Right. So you are saying it is a perception that there is an increased error rate among people of color, or have we seen some data, although not significant, to show that?

Mr. WAGNER. I think the studies that have shown there were these biases in it had different control factors than how we are using this program. No one has really studied the way that we are implementing this using those same control factors on how we are doing it, and I would expect them to get the similar results as to we are seeing.

Mrs. DEMINGS. Mr. Gould, can you——

Mr. GOULD. Ma'am, from a TSA perspective, we work very closely with the DHS Science and Technology Director as well. They inform our test plans and how we collect data on the biometric pilots and how well they are working, and then they analyze that data on our behalf. So we really do rely on them for their semi-independent and very, very accurate assessments of our capability.

Then, like CBP, we rely on our friends at NIST as well to, you know, really set the standards and say how well the algorithms are actually working.

Mrs. DEMINGS. So when you decide—Mr. Chairman, if I could just—when you decide that this—we are ready for deployment, this technology, based on the testing we have done, is ready for prime time, who makes that decision? Is it a collective effort between the different people that you work with, or do you decide that individually based on the feedback that you receive?

Mr. WAGNER. We would decide that for our agency, because it is our responsibility. The officer's determination, you match your passport, and if I use a tool or an algorithm to help me make that decision, at the end of the day, it is still my judgment to do that. So we would evaluate this to say, is this helpful to the officer making that determination, that this document corresponds to that person.

Mrs. DEMINGS. OK.

Mr. GOULD. One thing I would add to your original point, for us, the main reason to do this is increased—better identity verification, right, and the secure enhancements that are associated with that. Getting people through the checkpoint more quickly, like you said, is kind of icing on the cake. But better security through using this technology is really, really key to us. If the algorithms and the match rates are not acceptable, if we are not enhancing security, then we will not deploy it, but that decision would be made internal at the TSA.

Mrs. DEMINGS. Thank you, Mr. Chair.

I yield back.

Mr. PAYNE. I thank the gentlelady, and I just—probably due to the time, I will dispense with my questions, but I would just like to say that obviously based on the questioning from the Members of Congress, you can get a feeling on where we are concerned about

issues around privacy, around equality, and making sure that the American people and the traveling public is safe. So we need to continue to evolve, and we know that Homeland Security has been an evolving, living, breathing entity that continues to have to see and recognize issues, try to curtail them, and rectify matters that are important to the American people.

So I would just like to say, thank you for your service in TSA, CBP. Your jobs, all of you actually, Secret Service, are doing a yeoman's job for this Nation, and we appreciate your service and your time here today, so thank you.

With that, the hearing is adjourned.

[Whereupon, at 12:18 p.m., the committee was adjourned.]