ASSESSING CBP'S USE OF FACIAL RECOGNITION TECHNOLOGY

HEARING

BEFORE THE

SUBCOMMITTEE ON BORDER SECURITY, FACILITATION, AND OPERATIONS

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

JULY 27, 2022

Serial No. 117–68

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
49–891 PDF WASHINGTON : 2022

COMMITTEE ON HOMELAND SECURITY

Bennie G. Thompson, Mississippi, *Chairman*

Sheila Jackson Lee, Texas
James R. Langevin, Rhode Island
Donald M. Payne, Jr., New Jersey
J. Luis Correa, California
Elissa Slotkin, Michigan
Emanuel Cleaver, Missouri
Al Green, Texas
Yvette D. Clarke, New York
Eric Swalwell, California
Dina Titus, Nevada
Bonnie Watson Coleman, New Jersey
Kathleen M. Rice, New York
Val Butler Demings, Florida
Nanette Diaz Barragán, California
Josh Gottheimer, New Jersey
Elaine G. Luria, Virginia
Tom Malinowski, New Jersey
Ritchie Torres, New York

John Katko, New York
Michael T. McCaul, Texas
Clay Higgins, Louisiana
Michael Guest, Mississippi
Dan Bishop, North Carolina
Jefferson Van Drew, New Jersey
Mariannette Miller-Meeks, Iowa
Diana Harshbarger, Tennessee
Andrew S. Clyde, Georgia
Carlos A. Gimenez, Florida
Jake LaTurner, Kansas
Peter Meijer, Michigan
Kat Cammack, Florida
August Pfluger, Texas
Andrew R. Garbarino, New York
Mayra Flores, Texas

Hope Goins, *Staff Director*
Daniel Kroese, *Minority Staff Director*
Natalie Nixon, *Clerk*

SUBCOMMITTEE ON BORDER SECURITY, FACILITATION, AND OPERATIONS

Nanette Diaz Barragán, California, *Chairwoman*

J. Luis Correa, California
Emanuel Cleaver, Missouri
Al Green, Texas
Yvette D. Clarke, New York
Bennie G. Thompson, Mississippi *(ex officio)*

Clay Higgins, Louisiana, *Ranking Member*
Dan Bishop, North Carolina
Andrew S. Clyde, Georgia
Mayra Flores, Texas
John Katko, New York *(ex officio)*

Brieana Marticorena, *Subcommittee Staff Director*
Natasha Eby, *Minority Subcommittee Staff Director*
Zachary Wood, *Subcommittee Clerk*

CONTENTS

Page

STATEMENTS

The Honorable Nanette Diaz Barragán, a Representative in Congress From the State of California, and Chairwoman, Subcommittee on Border Security, Facilitation, and Operations:
Oral Statement 1
Prepared Statement 2
The Honorable Clay Higgins, a Representative in Congress From the State of Louisiana, and Ranking Member, Subcommittee on Border Security, Facilitation, and Operations 3
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Chairman, Committee on Homeland Security:
Prepared Statement 7

WITNESSES

Ms. Rebecca Gambler, Director, Homeland Security and Justice, U.S. Government Accountability Office (GAO):
Oral Statement 8
Prepared Statement 10
Mr. Jeramie D. Scott, Senior Counsel, Electronic Privacy Information Center (EPIC):
Oral Statement 21
Prepared Statement 22
Ms. Nicol Turner Lee, PhD, Director, The Center for Technology Innovation (CTI), The Brookings Institution:
Oral Statement 32
Prepared Statement 33
Mr. Daniel P. Tanciar, Chief Innovation Officer, Pangiam:
Oral Statement 44
Prepared Statement 46

FOR THE RECORD

The Honorable Clay Higgins, a Representative in Congress From the State of Louisiana, and Ranking Member, Subcommittee on Border Security, Facilitation, and Operations:
Letter, Security Industry Association 4
Letter, Airlines for America 5

ASSESSING CBP'S USE OF FACIAL RECOGNITION TECHNOLOGY

Wednesday, July 27, 2022

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON BORDER SECURITY,
FACILITATION, AND OPERATIONS,
Washington, DC.

The subcommittee met, pursuant to notice, at 2 p.m., in room 310, Cannon House Office Building, Hon. Nanette Diaz Barragán [Chairwoman of the Subcommittee] presiding.

Present: Representatives Barragán, Cleaver, Clarke, Higgins, and Flores.

Chairwoman BARRAGÁN. The Subcommittee on Border Security Facilitation and Operations will come to order. Thank you for joining today's hearing to assess U.S. Customs and Border Protection's use of facial recognition technology. CBP tested several types of biometric technologies, including hand-held fingerprint scanning devices and iris scanning, before deciding to pursue facial recognition technology as its biometric capability. Facial recognition technology uses a computer algorithm to compare a picture taken in person at the airport or other border checkpoints to the traveler's passport picture or visa.

This technology cannot only be a powerful tool for homeland security, but can also help facilitate travel. However, the use of facial recognition technology raises questions about data privacy and how passengers' information is used and stored. It also raises questions about the adequacy of the oversight mechanisms in place. For example, although CBP policy does not allow airlines and partners to store passengers' photos, the agency does not have a robust system for conducting audits. These audits are vital to building public trust.

Proper oversight ensures that biometric data gathered in airports is not monetized by private industry or kept in industry databases. Potential bias in identification is also a significant concern, particularly when a technology affects various races, age groups, and gender differently.

In 2019, a National Institute of Standards and Technology, NIST, report found that Asian and African American faces were 10 to 100 times more likely to be misidentified than white faces. The report also found that children and elderly people were more likely to be misidentified than middle-aged people, and women were more likely to be misidentified than men. NIST also found that the best-performing algorithms had undetectable differences in performance across demographic groups. Though this sounds promising, the report tested algorithms, not the system as a whole. These systems include the environment where the technology is deployed and the cameras that capture facial images. Lighting and image quality can have a significant impact on the success of the technology.

We have also heard concerns about potential mission creep in the Department's use of biometric data. Current authorized uses are set by policy and guidance, which are more open to change than laws, rules, and regulations. Understanding CBP's use of facial recognition technology and the issues and concerns surrounding its use is crucial to our responsibility to conduct oversight.

Two weeks ago, Members of this subcommittee were briefed by Government officials from Customs and Border Protection, the Department of Homeland Security's Office of Civil Rights and Civil Liberties, and the National Institute of Standards and Technology on CBP's use of facial recognition technology and the safeguards in place to protect privacy. The briefing served as an opportunity for Members to learn more about the technology and how it is being deployed.

It was also an opportunity for Members to ask questions and raise concerns regarding privacy and bias. During the briefing, we learned that Simplified Arrival has been rolled out with facial recognition technology in all U.S. international airports. This is the system travelers use when entering the United States.

We also learned that biometric exit systems using facial recognition are active in only 26 airports. CBP continues to expand the use of facial recognition technology across airports as well as sea and land ports of entry.

Today, we will have the opportunity to continue our conversation on CBP's use of facial recognition technology with experts from the U.S. Government Accountability Office, the Electronic Privacy Information Center, the Brookings Institution, and Pangiam. Did I say that right, Pangiam? Our witnesses will discuss CGP's deployment of facial recognition technology as well as the implications related to accuracy, bias, and privacy in verifying traveler identities.

I look forward to a frank conversation on CBP's use of facial recognition technology and how Congress can conduct meaningful oversight.

With that, the Chair now recognizes the Ranking Member of the subcommittee, Mr. Higgins of Louisiana, for an opening statement.

[The statement of Chairwoman Barragán follows:]

STATEMENT OF CHAIRWOMAN NANETTE BARRAGÁN

JULY 27, 2022

CBP tested several types of biometric technologies, including handheld fingerprint-scanning devices and iris scanning, before deciding to pursue facial recognition technology as its biometric capability. Facial recognition technology uses a computer algorithm to compare a picture taken in person at the airport or other border checkpoints to the traveler's passport picture or visa.

This technology cannot only be a powerful tool for homeland security but can also help facilitate travel. However, the use of facial recognition technology raises questions about data privacy and how passengers' information is used and stored. It also raises questions about the adequacy of the oversight mechanisms in place. For example, although CBP policy does not allow airlines and partners to store passengers' photos, the agency does not have a robust system for conducting audits.

These audits are vital to building public trust. Proper oversight ensures that biometric data gathered in airports is not monetized by private industry or kept in industry databases. Potential bias in identification is also a significant concern, particularly when a technology affects various races, age groups, and genders differently.

In 2019, a National Institute of Standards and Technology (NIST) report found that Asian and African American faces were 10 to 100 times more likely to be misidentified than white faces. The report also found that children and elderly people were more likely to be misidentified than middle-aged people, and women were more likely to be misidentified than men. NIST also found that the best-performing algorithms had "undetectable" differences in performance across demographic groups. Though this sounds promising, the report tested algorithms, not the system as a whole. These systems include the environment where the technology is deployed and the cameras that capture facial images. Lighting and image quality can have a significant impact on the success of the technology.

We've also heard concerns about potential "mission creep" in the Department's use of biometric data. Current authorized uses are set by policy and guidance, which are more open to change than laws, rules, and regulations. Understanding CBP's use of facial recognition technology and the issues and concerns surrounding its use is crucial to our responsibility to conduct oversight.

Two weeks ago, Members of the subcommittee were briefed by Government officials from Customs and Border Protection, the Department of Homeland Security's Office of Civil Rights and Civil Liberties, and the National Institute of Standards and Technology on CBP's use of facial recognition technology and the safeguards in place to protect privacy. The briefing served as an opportunity for Members to learn more about the technology and how it is being deployed. It was also an opportunity for Members to ask questions and raise concerns regarding privacy and bias. During the briefing, we learned that Simplified Arrival has been rolled out with facial recognition technology in all U.S. international airports. This is the system travelers use when entering the United States. We also learned that biometric exit systems using facial recognition are active in only 26 airports. CBP continues to expand the use of facial recognition technology across airports, as well as at sea and land ports of entry.

Today, we will have the opportunity to continue our conversation on CBP's use of facial recognition technology with experts from the U.S. Government Accountability Office (GAO), the Electronic Privacy Information Center (EPIC), the Brookings Institution, and Pangiam. Our witnesses will discuss CBP's deployment of facial recognition technology as well as the implications related to accuracy, bias, and privacy in verifying traveler identities.

Mr. HIGGINS. Thank you, Madam Chair, for holding today's hearing. I also thank our witnesses for appearing before us today. I thank my colleagues for attending in person or virtually.

This is a topic that Republicans and Democrats are not that far apart on. The final yards of this struggle seem to be challenging, but facial recognition technology is certainly an emerging asset in this digital realm and wherein it can be properly deployed and effectively deployed to help our Nation protect its sovereignty and protect our travelers in their journeys. We are moving effectively forward through Congressional oversight on this committee to determine exactly in what manner shall Congress embrace this technology. I think it is a pretty much accepted conclusion that it is an effective asset that we should embrace and use, but with proper restraints and controls.

Madam Chair, I have a letter to this committee from the Security Industry Association regarding the effectiveness of facial recognition technology, a letter to the committee from Airlines for America essentially stating the same, and a report from the National Institute of Standards and Technology through the U.S. Department of

Commerce* regarding biometric service systems and their efficiency I would like to submit for the record.

Chairwoman BARRAGÁN. Without objection.

[The information follows:]

July 27, 2022.

The Honorable NANETTE BARRAGÁN,
Chairwoman, Subcommittee on Border Security, Facilitation & Operations, House Committee on Homeland Security, 2246 Rayburn House Office Building, Washington, DC 20515.

The Honorable CLAY HIGGINS,
Ranking Member, Subcommittee on Border Security, Facilitation & Operations, House Committee on Homeland Security, 572 Cannon House Office Building, Washington, DC 20515.

DEAR CHAIRWOMAN BARRAGÁN AND RANKING MEMBER HIGGINS: On behalf of the Security Industry Association (SIA), thank you for holding a hearing on U.S. Customs and Border Protection's (CBP's) use of facial recognition technologies.

SIA represents over 1,000 companies that provide technology solutions vital to bolstering National security, promoting public safety, and protecting information and critical infrastructure. SIA believes all technologies, including facial recognition technologies, must only be used for purposes that are lawful and ethical, and SIA has published principles to promote the responsible and effective use of facial recognition technologies.

The benefits of facial recognition technologies are proven and growing across a wide range of use cases and functional applications. In the United States, facial recognition technologies have helped detect identity fraud that fuels other criminal activity, find and rescue human trafficking victims, thwart potential terrorist attacks, solve hate crimes, and crack cold cases.[1] Furthermore, as previous hearings have established, the Department of Homeland Security's (DHS's) use of facial recognition technologies helps promote national security and public safety and helps enable smoother and more efficient travel in a privacy-protective manner.[2] CBP has deployed facial recognition technologies at 238 airports for air entry (including all international airports in the U.S. and all 14 Preclearance locations worldwide), 32 airports for air departure, 26 seaports, and all pedestrian lanes at ports of entry along the northern and southern land borders.[3] Through the use of highly accurate facial recognition technologies, CBP has processed over 193 million travelers, confirmed more than 163,000 visa overstays, and prevented over 1,500 imposters from entering the United States at air and land ports under false identities.

Algorithm testing by the National Institute of Standards and Technology (NIST) and full system testing by the Department of Homeland Security's Science & Technology Directorate (DHS S&T) show that facial recognition technologies are rapidly becoming more and more accurate—often achieving accuracy rates >99 percent[4]—and DHS's facial recognition technology providers continue to rank among the most accurate in these tests. NIST's December 2019 FRVT Part 3: Demographic Effects report found that a version of the algorithm that DHS currently deploys had "undetectable" false positive error rate differentials across demographic groups based on skin tone and sex,[5] and CBP has testified that it does not see demo-

* The report has been retained in committee files and is available at *https://doi.org/10.6028/NIST.IR.8381*.

[1] For more information, see *https://www.securityindustry.org/2020/07/16/facial-recognition-success-stories-showcase-positive-use-cases-of-the-technology/*.

[2] During the February 6, 2020, House Committee on Homeland Security hearing entitled "About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II," Representative Walker asked John Wagner, the witness from Customs and Border Protection, if it was "true that the Biometric Entry/Exit system uses less personally identifiable information than the current system that we have in place?" Mr. Wagner responded, "Yes, because currently . . . you're exposing your name, your date of birth, your passport number, your place of birth—all the information on your passport page . . . You're disclosing it to a person who doesn't actually need to know all of that additional information versus standing in front of a camera with no identifiable information other than your face, which they can already see—and your picture is taken, and on the screen comes a green checkmark and that person now knows you've been validated by the Government record to proceed. So you're sharing actually, less information in this instance."

[3] *https://biometrics.cbp.gov/*.

[4] *https://pages.nist.gov/frvt/html/frvt1N.html; https://mdtf.org/Rally2021/Results2021*.

[5] National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (NISTIR 8280), p. 8, *https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf*.

graphic-based error rates in its operations.[6] Furthermore, a September 2020 report by the Government Accountability Office found that air exit, which is part of the Congressionally-mandated Biometric Entry-Exit program, "met or exceeded its two accuracy requirements—specifically, for the true and false acceptance rates."[7]

SIA recognizes and commends the benefits that DHS's use of facial recognition technologies has already produced. We also understand that legislation governing the Federal Government's procurement and use of facial recognition technologies could help build public trust and provide additional safeguards, and we support efforts to develop use-case-specific legislation that helps mitigate the risks and promote the numerous, wide-ranging benefits that facial recognition technologies can produce. Before considering legislation that would impact the use of facial recognition technologies, we encourage Members to review SIA's facial recognition technology resources, including *Principles for the Responsible and Effective Use of Facial Recognition Technology, What NIST Data Shows About Facial Recognition and Demographics,* and *Face Facts: How Facial Recognition Makes Us Safer & the Dangers of a Blanket Ban.*

SIA and our members appreciate and welcome opportunities to contribute to the on-going dialog about facial recognition technologies and associated policy issues and governance approaches. Please let us know if there is any way we can be of assistance as you continue to examine these issues.

Sincerely,

DON ERICKSON,
CEO, Security Industry Association.

July 26, 2022

The Honorable NANETTE BARRAGÁN,
Chairwoman, Subcommittee on Border Security, Facilitation, & Operations, House Committee on Homeland Security, U.S. House of Representatives, 2246 Rayburn House Office Building, Washington, DC 20515.

The Honorable CLAY HIGGINS,
Ranking Member, Subcommittee on Border Security, Facilitation, & Operations, House Committee on Homeland Security, U.S. House of Representatives, 572 Cannon House Office Building, Washington, DC 20515.

DEAR CHAIRWOMAN BARRAGÁN AND RANKING MEMBER HIGGINS: On behalf of our member carriers, Airlines for America (A4A) appreciates the opportunity to provide our perspective on facial recognition technology. Identity verification is a cornerstone of aviation security and facilitation, and our member airlines [1] have worked closely with the Department of Homeland Security (DHS) for over 10 years to support evaluation, testing, and fielding of biometric technologies including facial recognition. The principal goals of this technology are to enhance security and improve the passenger experience while ensuring the highest levels of privacy and transparency.

As you are aware, U.S. Customs and Border Protection (CBP) is implementing facial recognition technology to comply with the congressional mandate to develop a biometric air entry/exit program for arriving and departing international air passengers. The Transportation Security Administration (TSA) is also evaluating facial recognition for identity verification at security checkpoints. It is critical to consider the unique use case of facial recognition technology in the air travel environment, as these tools simply automate a mandatory manual process.

Airlines serve customers globally. We recognize the importance of accuracy in facial recognition algorithmic performance across all ethnicities and genders. Inaccuracy rates, even at small percentages, have outsized impacts on populations as large and diverse as air travel passengers. False negatives and false positives in the air travel environment can undermine the government's ability to fulfill its security mission, undercut carriers' ability to confer benefits and facilitate the passenger ex-

[6] During the February 6, 2020, House Committee on Homeland Security hearing, John Wagner said, "Well, again, we're using a high-performing algorithm that we're not seeing those demographic-based error rates."

[7] Government Accountability Office, *CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues,* GAO–20–568 (September 2020), p. 51, *https://www.gao.gov/assets/gao-20-568.pdf.*

[1] A4A is the principal trade and service organization of the U.S. scheduled airline industry. Members of the association are Alaska Airlines, Inc.; American Airlines Group, Inc.; Atlas Air, Inc.; Delta Air Lines, Inc., Federal Express Corporation; Hawaiian Airlines; JetBlue Airways Corp.; Southwest Airlines Co.; United Holdings, Inc.; and United Parcel Service Co. Air Canada is an associate member.

perience and tax operational resources for government and industry alike. High inaccuracy rates, therefore, do not scale for the security or airline use cases for biometrics.

We are therefore encouraged by the tremendous technological strides in industry and the commitment of our DHS partners to ensuring accuracy in facial matching. A 2019 National Institute of Standards and Technology (NIST) report on the performance of facial recognition algorithms across different demographic groups shows that the development of this technology is already highly accurate and improving.[2] The most accurate algorithms achieved greater accuracy than humans. Algorithms refined during the pandemic showed increased matching rates of masked passengers to the pre-pandemic algorithms, according to NIST.[3] We applaud the facial recognition industry's rapid adaptability and overall commitment to continuous improvement.

Privacy and security of our passengers' biometric data is also of the utmost concern. Automated facial matching has privacy and data security protections built in to protect the biometric information in-transit and at-rest. As required by DHS when using DHS matching capability, photos taken for the purpose of automated facial matching are purged by air carriers following their secure verification by DHS. Airline connections to secure, encrypted DHS systems for verification ensure passenger data is protected in-transit.

We work with DHS to educate passengers on how the technology is used and which personal data elements are shared or stored. All these steps are key to encourage passenger acceptance and to achieve operational benefits of 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.

We commend CBP for moving forward with the deployment of Simplified Arrival at all major airports of entry during the pandemic. As international arrivals continue to increase, Simplified Arrival is helping to prevent congestion and long lines within the Federal Inspection Station (FIS) during peak arrival times. Additionally, we applaud CBP's deployment of facial recognition technology for the Global Entry Trusted Traveler program. Upgrading the Global Entry kiosks to eliminate the need to provide fingerprints and rely on facial recognition technology has also helped to prevent congestion.

We value our ongoing collaboration with DHS as the Department and its component agencies further deploy facial recognition technology in air travel 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.

Sincerely,

LAUREN BEYER,
Vice President, Security and Facilitation.

Mr. HIGGINS. Thank you, Madam Chair. Over the last several years, biometric technology has improved significantly. We all recognize this, the technological advance of facial recognition tech should not be a surprised. Most of us here do not have the same iPhone in our pocket that we had 2 or 3 years ago, much less 10 years ago. So, some of the challenges and algorithm issues and recognition concerns that originally became part of the narrative of facial recognition technology were completely reasonable assessments of the technology at the time. But the industry has advanced the tech and it is an effective tool.

Our border agents who are not with us today, though they should be, have asked for this technology to help them not just with rec-

[2] Grother, P., Ngan, M., and Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. NIST.IR 8280. Available at: *https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.*

[3] Ngan, M., Grother, P. and Hanaoka, K. (2020), Ongoing Face Recognition Vendor Test (FRVT) Part 6B: Face recognition accuracy with face masks using post-COVID–19 algorithms. NIST.IR.8331. Available at: *https://doi.org/10.6028/NIST.IR.8331.*

ognition, but with streamlining the entry process. At our ports of entry it is not uncommon that you have foot traffic that comes across from Mexico. These are Mexican citizens that have earned their living by essentially shopping for their neighbors in their community. They walk across. I have been there and visited with them and the bottom line is that as the cartels have strengthened their criminal efforts, their trafficking at the border, the United States has been forced to respond with more stringent vetting at our ports of entry, including the foot traffic that comes across.

These are just, you know, squared away, law-abiding Mexican citizens that are earning a little living shopping for their neighbors and friends. They walk across, they buy some stuff, they go back. But because the vetting is required to be more stringent due to the cartels' criminal operations, the lines take longer, so they can only make—it may be a line for 4 hours now whereas years ago you were only in line for maybe 45 minutes. So, they can only make maybe 1 or 2 trips a day instead of 3 or 4. So, it has had an economic impact on our fellow children of God and our neighbors across the border.

Facial recognition technology could absolutely be deployed to those ports of entry where the foot traffic coming through would roll right through. If they were not recognized, then they would be pulled from the line, or they had a random check, they would go through the human verification that is currently a requirement.

So, the deployment of this technology is something that we should carefully consider and control and we should also embrace and recognize that it has advanced tremendously since its introduction and our awareness of it over the course of the last decade.

Madam Chair, I thank you for holding this hearing and I look forward to questioning the panelists today.

Chairwoman BARRAGÁN. Thank you, Mr. Ranking Member. Other Members are reminded that stateents may be submitted for the record.

[The statement of Chairman Bennie G. Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

JULY 27, 2022

Today's discussion is an opportunity to better understand how CBP uses facial recognition technology to secure the homeland and the measures or policies in place to ensure people's privacy is protected. It is also an important opportunity to further understand the concerns surrounding bias in the use of the technology. The committee has followed this topic closely for a long time.

In 2019 and 2020, we held hearings with representatives from CBP, the Transportation Security Administration, the DHS Office of Civil Rights and Civil Liberties, the U.S. Secret Service, as well as the National Institute of Standards and Technology. At that time, several DHS components were in the process of expanding their use of facial recognition technology. These two hearings provided insight into the Department's plan to use biometric technology to automate traveler processing while increasing security. Facial recognition technology has improved since then.

Industry continues to enhance the accuracy, speed, and performance of the systems and algorithms used by the Federal Government. DHS has also significantly expanded its rollout. CBP has now fully deployed facial recognition technology for travelers entering the United States at all international airports. In addition, 26 airports are now using this technology for individuals departing the United States. Despite these advances, concerns regarding privacy and bias remain.

I am troubled that CBP has not yet ensured that travelers are appropriately notified of their ability to opt out of using the facial recognition technology. I visited a biometric exit gate in Las Vegas earlier this year, and no such signage was present. CBP and airport stakeholders must post proper signage notifying travelers of their ability to opt out. CBP must also ensure that facial recognition systems and algorithms do not lead to biased outcomes based on the race, gender, or age.

As facial biometric technology becomes more common, we must continue to examine the agency's implementation and implications of its use. Our witnesses today have closely tracked CBP's deployment of facial recognition technology. I look forward to their insights about the issues surrounding CBP's current and future plans for this technology.

Chairwoman BARRAGÁN. I now would like to welcome our panel of witnesses.

Rebecca Gambler is the director of the Government Accountability Office's Homeland Security and Justice team. In her role Ms. Gambler leads GAO's work on a myriad of topics, including border security efforts and technology deployments along the Southern Border.

Jeramie Scott is senior counsel at the Electronic Privacy Information Center. Mr. Scott's work focuses on the nexus between surveillance technology such as facial recognition technology and privacy issues. He is with us remotely.

Nichol Turner Lee is the director of the Center for Technology Innovation at The Brookings Institution. Dr. Turner Lee is an expert in the intersection of race, wealth, and technology within the context of civic engagement, criminal justice, and economic development. She is also with us remotely.

Daniel Tanciar is the chief innovation officer at Pangiam. He previously served as the executive director of planning, program analysis, and evaluation in the Office of Field Operations, Customs and Border Protection, where he helped advance CBP's biometric exit and entry system.

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

I now will ask each witness to summarize his or her statement for 5 minutes beginning with Ms. Rebecca Gambler.

STATEMENT OF REBECCA GAMBLER, DIRECTOR, HOMELAND SECURITY AND JUSTICE, U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO)

Ms. GAMBLER. Good afternoon, Chairwoman Barragán, Ranking Member Higgins, and Members of the subcommittee. Thank you for the opportunity to testify at today's hearing to discuss GAO's work on CBP's use of facial recognition technology at ports of entry as part of its biometric entry/exit program.

Beginning in 1996, a series of Federal laws has required CBP to develop and implement a biometric entry-exit system to match arrival and departure records of foreign nationalists. Since 2004, CBP has implemented a biometric entry system. However, we have identified long-standing challenges to CBP developing and deploying a biometric exit capability.

Over the years, CBP has tested various biometric technologies to determine which type of technology could be deployed on a large scale without disrupting travel and trade. Based on the results of its testing, CBP concluded that facial recognition technology was the most operationally feasible and traveler-friendly option.

CBP has partnered with airlines and airports to deploy facial recognition technology to at least one gate at 32 airports for travelers exiting the United States and at all airports for travelers entering the country. It has also deployed the technology at 26 seaports for travelers entering the United States. At land ports of entry CBP has deployed facial recognition technology at all 159 land ports for pedestrians entering the United States, and is in the early stages of pilot testing the technology for other areas of the land environment.

GAO has issued numerous reports on CBP's efforts to develop and deploy a biometric entry-exit system. Today I will summarize our most recent report on this topic from September 2020, which focused on CBP's use of facial recognition technology. In particular, I will highlight two key findings from that report.

First, CBP's Biometric Entry-Exit Program has incorporated some privacy principles by, for example, prohibiting partners like air carriers from storing travelers' photos and providing public notices on privacy protections. However, CBP notices have not always been current, complete, or available, and have provided limited information on how to request to opt out of facial recognition. For example, at the time of our review, CBP's public website on the program did not accurately reflect the locations where CBP used or tested facial recognition technology. Therefore, travelers who check the website would not see a complete list of locations where they may encounter the technology.

In another example, during one of our airport visits, an airline was using facial recognition technology at a gate, but there were no privacy signs posted. Further, while CBP allows eligible travelers to request to opt out of facial recognition identity verification, the CBP notices we observed provided limited information on the process for opting out. We recommended that CBP ensure its privacy notices contain complete and current information, and that the privacy signage is consistently available at all locations.

CBP implemented that first recommendation by, for example, creating a new website that outlines the locations where CBP uses facial recognition. For the second recommendation CBP has reviewed its language on signs and is in the process of updating them, but CBP needs to complete those efforts.

Second, CBP requires its commercial partners, contractors, and vendors to follow CBP's data collection and privacy requirements such as restrictions on retaining or using traveler photos for their own use. CBP can conduct audits to assess their compliance. However, at the time of our review CBP had audited only one of its airline partners and did not have a plan to ensure that all partners, contractors, and vendors are audited for compliance.

We recommended that CBP develop and implement a plan to conduct privacy audits at its commercial partners, contractors, and vendors. Since our report, CBP has completed additional audits of its airline partners and has others planned or under way. This is positive, but CBP needs to complete those assessments and audit partners in the sea and land environments as well as vendors and contractors who have access to personally identifiable information.

In closing, CBP has made progress in deploying facial recognition for traveler identification and verification, and is addressing some privacy considerations. But additional action is needed to fully implement our remaining recommendations and we will continue to monitor CBP's efforts to address those recommendations.

This concludes my prepared statement and I am happy to answer any questions the committee Members may have.

[The prepared statement of Ms. Gambler follows:]

Prepared Statement of Rebecca Gambler

Wednesday, July 27, 2022

GAO HIGHLIGHTS

Highlights of GAO–22–106154, a testimony before the Subcommittee on Border Security, Facilitation, and Operations, Committee on Homeland Security, House of Representatives.

Why GAO Did This Study

Within the Department of Homeland Security (DHS), CBP is charged with the dual mission of facilitating legitimate travel and securing U.S. borders. Federal laws require DHS to implement a biographic and biometric data system for foreign nationals entering and exiting the United States. In response, CBP has been pursuing FRT to verify a traveler's identity in place of a visual inspection of travel identification documents.

This statement addresses the extent to which CBP has: (1) Incorporated privacy principles in and (2) assessed the accuracy and performance of its use of FRT. This statement is based on a September 2020 report (GAO–20–568), along with updates as of July 2022 on actions CBP has taken to address prior GAO recommendations. For that report, GAO conducted site visits to observe CBP's use of FRT; reviewed program documents; and interviewed DHS officials.

What GAO Recommends

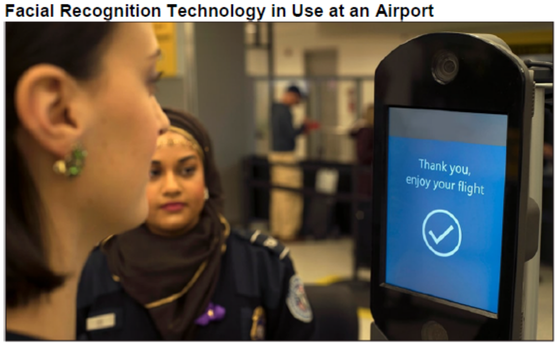
In September 2020, GAO made five recommendations to CBP regarding privacy and system performance of its FRT. DHS concurred with the recommendations and has implemented two of them. CBP is taking steps to address the remaining three recommendations related to: (1) Current and complete privacy signage, (2) implementing an audit plan for its program partners, and (3) capturing required traveler photos.

FACIAL RECOGNITION TECHNOLOGY.—CBP TRAVELER IDENTITY VERIFICATION AND EFFORTS TO ADDRESS PRIVACY ISSUES

What GAO Found

U.S. Customs and Border Protection (CBP) has made progress testing and deploying facial recognition technology (FRT) at air, sea, and land ports of entry to create entry-exit records for foreign nationals as part of its Biometric Entry-Exit Program. As of July 2022, CBP has deployed FRT at 32 airports to biometrically confirm travelers' identities as they depart the United States (air exit) and at all airports for arriving international travelers.

Facial Recognition Technology in Use at an Airport



Source: U.S. Customs and Border Protection. | GAO-22-106154

In September 2020, GAO reported that CBP had incorporated privacy principles in its program, such as prohibiting airlines from using travelers' photos for their own purposes. However, CBP had not consistently provided travelers with information about FRT locations. Also, CBP's privacy signage provided limited information on how travelers could request to opt out of FRT screening and were not always posted. Since that time, CBP has ensured that privacy notices contain complete information and is taking steps to ensure signage is more consistently available, but needs to complete its efforts to update signs in locations where FRT is used. Further, CBP requires its commercial partners, such as airlines, to follow CBP's privacy requirements and could audit partners to assess compliance. As of May 2020, CBP had audited one airline partner and did not have a plan to ensure all partners were audited. In July 2022, CBP reported that it has conducted five assessments of its air partners and has three additional assessments under way. These are positive steps to help ensure that air traveler information is safeguarded. However, CBP should also audit other partners who have access to personally identifiable information, including contractors and partners at land and sea ports of entry.

CBP assessed the accuracy and performance of air exit FRT capabilities through operational testing. Testing found that air exit exceeded its accuracy goals but did not meet a performance goal to capture 97 percent of traveler photos. As of July 2022, CBP officials report that they are removing the photo capture goal because airline participation in the program is voluntary and CBP does not have staff to monitor the photo capture process at every gate.

Chairwoman Barragán, Ranking Member Higgins and Members of the subcommittee: I am pleased to be here today to discuss our work on U.S. Customs and Border Protection's (CBP) use of facial recognition technology (FRT) at ports of entry.[1] FRT has become increasingly common across business and Government as a tool for identifying or verifying customers or persons of interest. Within the Department of Homeland Security (DHS), CBP is the lead Federal agency charged with the dual mission of facilitating legitimate trade and travel at our Nation's borders while also keeping terrorists and their weapons, criminals and contraband, and other inadmissible individuals out of the country. As part of this mission, Federal laws require DHS to implement a biographic and biometric data system for foreign nationals entering and exiting the United States. In response to these laws, CBP has been pursuing FRT to automatically verify a traveler's identity in place of a visual inspection of travel identification documents.[2] Traditionally, CBP has relied on biographic information (i.e., name or date of birth) on travel documents to verify that a traveler is who they claim to be. According to CBP, automating the identity verification process using FRT helps increase their ability to detect fraudulent travel identification documents, as well as expedite identity verification processes.

CBP officers are responsible for inspecting international travelers—including foreign nationals and U.S. citizens—arriving at ports of entry. Officers review travelers' identification documents, including passports, visas, or other entry permits, to verify their identities; determine their admissibility to the United States; and create entry records, among other things. Additionally, CBP is responsible for confirming foreign national departures from the United States to determine if their exit occurred by expiration of the authorized period of stay as defined by their temporary status.

[1] Ports of entry are facilities that provide for the controlled entry into or departure from the United States. Specifically, a port of entry is any officially designated location (seaport, airport, or land border location) where CBP officers clear passengers, merchandise and other items; collect duties; enforce customs laws; and inspect persons entering or applying for admission into the United States pursuant to U.S. immigration and travel controls.

[2] Under 8 U.S.C. § 1365b(d), the entry and exit data system is to require the collection of biometric exit data for all categories of individuals who are required to provide such entry data, regardless of the port of entry. For categories of individuals required to provide biometric entry and departure data, see 8 C.F.R. §§ 215.8 (DHS authority to establish pilot programs at land ports and at up to 15 air or sea ports, requiring biometric identifiers to be collected from foreign nationals on departure from the United States) 235.1(f) (any foreign national may be required to provide biometric identifiers on entry, except certain Canadian tourists or businesspeople; foreign nationals younger than 14 or older than 79; and diplomatic visa holders, among other listed exemptions. Additionally, foreign nationals required to provide biometric identifiers on entry may be subject to departure requirements for biometrics under § 215.8, unless otherwise exempted). We use the term foreign national in this statement to refer to someone who does not have U.S. citizenship or nationality seeking entry into the United States on a temporary basis pursuant to a nonimmigrant category (i.e. foreign visitor), such as tourists, diplomats, international students, or exchange visitors, among other types of nonimmigrant travelers. Lawful permanent residents are also in-scope for biometric collection and included in the definition of foreign nationals.

Beginning in 1996, a series of Federal laws were enacted to develop and implement an entry-exit data system, which is to integrate biographic and, since 2004, biometric records of foreign nationals entering and exiting the country and identify overstays.[3] Since 2004, DHS has tracked foreign nationals' entries into the United States as part of an effort to comply with legislative requirements and, since December 2006, a biometric entry capability has been fully operational at all air, sea, and land ports of entry. However, in previous reports we have identified long-standing challenges to DHS developing and deploying a biometric exit capability to create biometric records for foreign nationals when they depart the country, such as differences in logistics and infrastructure among ports of entry.[4]

To meet the requirement to implement a biometric exit capability, over the years CBP has tested various biometric technologies in different locations to determine which type of technology could be deployed on a large scale without disrupting legitimate travel and trade.[5] Based on the results of its testing, CBP concluded that FRT was the most operationally feasible and traveler-friendly option for a comprehensive biometric solution for travelers departing the United States, as well as those entering. Since then, CBP has prioritized testing and deploying FRT for departing and arriving travelers at airports (referred to, respectively, as air exit and air entry), with seaports and land ports of entry to follow. These tests and deployments are part of CBP's Biometric Entry-Exit Program.

As of July 2022, CBP has partnered with airlines and airport authorities to deploy FRT to at least one gate at 32 airports for travelers exiting the United States (air exit) and to all airports for travelers entering the United States (air entry), according to CBP officials.[6] With regard to the sea environment, CBP has deployed FRT at 26 seaports for travelers entering the United States (sea entry). With regard to the land environment, CBP has deployed FRT at all 159 land ports of entry for pedestrians entering the United States (land entry), and is in the early stages of pilot testing FRT for travelers entering the United States in vehicles and departing the United States as pedestrians or in vehicles (land exit). Figure 1 shows examples of cameras used for air exit facial recognition.

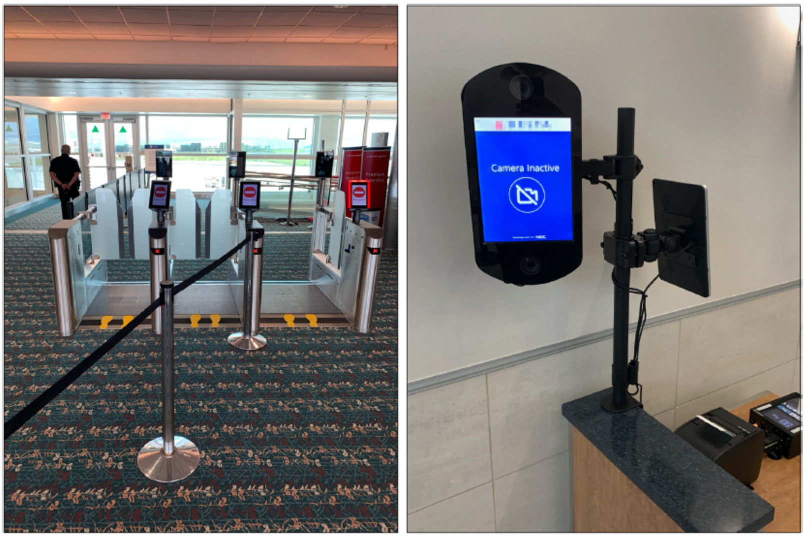
[3] 8 U.S.C. § 1365b, 8 C.F.R. § § 215.8, 235.1. A foreign national in the United States on a temporary basis who remains in the country beyond their authorized period of admission is classified as an overstay. A foreign national overstays by: (1) Failing to depart by the status expiration date or completion of qualifying activity (plus any time permitted for departure) without first obtaining an extension or other valid immigration status or protection, or (2) violating the terms and conditions of their visitor status at any point during their stay. Certain individuals are allowed to seek admission without a visa, such as citizens of Canada, as well as participants in the Visa Waiver Program, through which nationals of certain countries may apply for admission to the United States as temporary visitors for business or pleasure without first obtaining a visa from a U.S. embassy or consulate abroad. See 8 U.S.C. § 1187; 8 C.F.R. §§ 212.1, 214.6(d), 217.1–217.7; 22 C.F.R. §§ 41.0–41.3.

[4] See, for example, GAO, *Border Security: DHS Has Made Progress in Planning for a Biometric Air Exit System and Reporting Overstays, but Challenges Remain,* GAO–17–170 (Washington, DC: Feb. 27, 2017) and *Border Security: Actions Needed by DHS to Address Long-Standing Challenges in Planning for a Biometric Exit System,* GAO–16–358T (Washington, DC: Jan. 20, 2016).

[5] Specifically, from 2014 to 2016, CBP tested facial recognition, iris scanning, and mobile fingerprint readers in simulated operational conditions at air and land ports of entry. CBP used the results from each test to gauge the feasibility of real-time biometric identification that is traveler-friendly and easy to deploy for travel industry partners.

[6] As of July 2022, CBP officials said that FRT was currently deployed for air exit at 26 airports. There are an additional 6 airports where FRT was piloted or previously deployed, but where it is not currently deployed or in use.

Figure 1: Examples of Cameras Used for Air Exit Facial Recognition



Source: GAO. | GAO-22-106154

In September 2020, we reported on CBP's efforts to develop its FRT capabilities at ports of entry, including the extent to which CBP incorporated privacy protection principles and assessed the accuracy and performance of its FRT.[7] My statement today will summarize information from that report, as well as actions CBP has taken, as of July 2022, to address our recommendations from the report. To conduct the work from the September 2020 report, we conducted site visits to observe CBP's use of FRT in all three travel environments—air, land, and sea; reviewed program documents; and interviewed DHS officials. More detailed information on our objectives, scope, and methodology is contained in our September 2020 report.

We conducted the work on which this statement is based in accordance with generally accepted Government auditing standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

BACKGROUND

How Facial Recognition Technology Works

FRT uses an image or video of a person's face to identify them or verify their identity. Facial recognition, like fingerprint-matching technology, is a form of biometric identification that measures and analyzes physical attributes unique to a person that can be collected, stored, and used to confirm the identity of that person. FRT uses a photo or a still from a video feed of a person and converts it into a template, or a mathematical representation of the photo.[8] For some facial recognition functions, if the technology detects a face, a matching algorithm then compares the template to a template from another photo and calculates their similarity.[9] Facial recognition matching generally falls into one of two types: The first, known as "one-

[7] GAO, *Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues,* GAO–20–568 (Washington, DC: Sept. 2, 2020).

[8] Templates are generated according to the vendor-provided algorithm, and it is very difficult, if not impossible, to convert back to the original photo.

[9] An algorithm is a set of rules that a computer or program follows to compute an outcome. Private companies have developed hundreds of facial recognition algorithms for a variety of uses. For more information on the commercial use of FRT see GAO, *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses,* GAO–20–522 (Washington, DC: July 13, 2020).

to-many" or "1:N" matching, compares a live photo against a number (N) of photos in a gallery to determine if there is a match (identification of a particular face among many photos). The second, known as "one-to-one" or "1:1" matching, compares a live photo to another photo of the same person (verification of a face against a source photo, such as a passport photo).

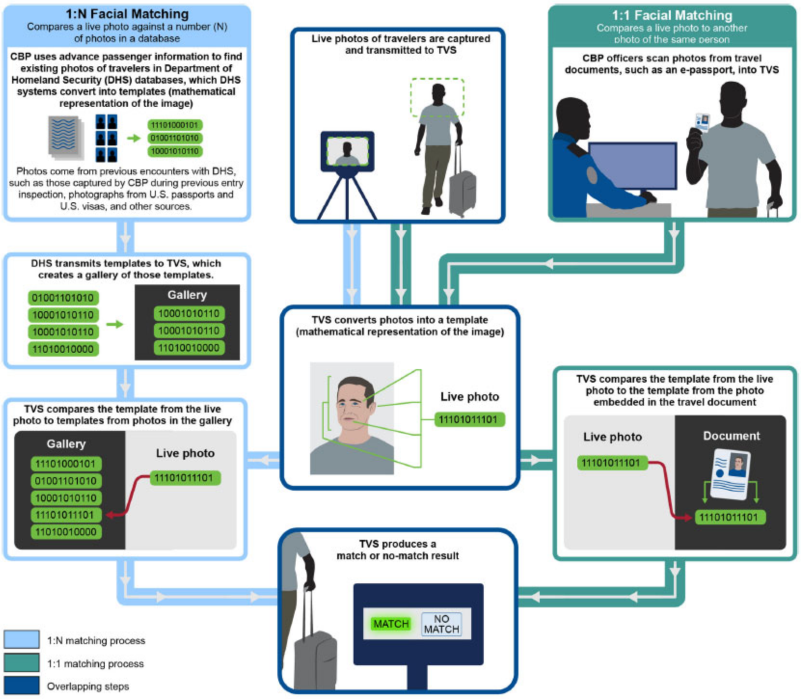
In 2017, CBP developed and implemented the Traveler Verification Service (TVS) as the facial recognition matching service for the Biometric Entry-Exit Program. Since then, CBP has been deploying TVS in segments based on the air, sea, and land travel environments at ports of entry.[10] TVS is a cloud-based service that uses an algorithm to compare live photos against existing photos and is designed to perform both 1:N and 1:1 facial recognition matching.

In the air and sea environments, CBP receives travelers' biographic information in advance of travel through passenger manifests submitted by aircraft operators and sea carriers. TVS searches DHS databases of photos associated with travelers listed on the manifest and then creates a pre-staged "gallery" of those photos.[11] These may include photos previously captured by CBP during entry inspections, photos from U.S. passports and U.S. visas, or photos from other DHS encounters. With 1:N matching, TVS compares a live photo of a traveler against photos of multiple travelers in the pre-staged gallery. For 1:1 matching, TVS electronically compares a live photo of a traveler against another photo of that traveler, such as a passport photo from their travel documents. This type of matching can be used when CBP does not have passenger manifest information or does not have an existing photo available for matching. Figure 2 shows how TVS performs facial matching.

[10] For example, beginning in 2017, CBP partnered with airlines and airport authorities to deploy facial recognition for identity verification at airport departure gates. CBP's program partners are responsible for purchasing the cameras to capture facial images from departing international travelers and facilitating the facial recognition identity verification process at gates.

[11] According to CBP officials, CBP has also begun creating galleries from commercial vehicle manifests at land ports of entry, as well as testing the feasibility of creating galleries of frequent border crossers.

Figure 2: Illustration of How CBP's Traveler Verification Service (TVS) Performs Facial Matching



1:N Facial Matching
Compares a live photo against a number (N) of photos in a database

CBP uses advance passenger information to find existing photos of travelers in Department of Homeland Security (DHS) databases, which DHS systems convert into templates (mathematical representation of the image)

Photos come from previous encounters with DHS, such as those captured by CBP during previous entry inspection, photographs from U.S. passports and U.S. visas, and other sources.

Live photos of travelers are captured and transmitted to TVS

1:1 Facial Matching
Compares a live photo to another photo of the same person

CBP officers scan photos from travel documents, such as an e-passport, into TVS

DHS transmits templates to TVS, which creates a gallery of those templates.

TVS converts photos into a template (mathematical representation of the image)

TVS compares the template from the live photo to templates from photos in the gallery

TVS compares the template from the live photo to the template from the photo embedded in the travel document

TVS produces a match or no-match result

🟦	1:N matching process
🟩	1:1 matching process
■	Overlapping steps

Source: GAO analysis of U.S. Customs and Border Protection information. | GAO-22-106154

CBP'S BIOMETRIC ENTRY-EXIT PROGRAM INCORPORATES SOME PRIVACY PROTECTION PRINCIPLES, BUT PRIVACY NOTICES AND AUDITS ARE INCONSISTENT

CBP's Privacy Notices to Inform the Public of Facial Recognition Contained Limited Privacy Information and Were Not Consistently Available

In our September 2020 report, we found that CBP's Biometric Entry-Exit Program incorporated some privacy protection principles consistent with the Fair Information Practice Principles DHS adopted, which serve as the basis for DHS's privacy policy.[12] For example, CBP's commercial partners, such as air carriers, are prohibited from storing or using travelers' photos for their own business purposes and can only view a match/no match result, which relate to the data use limitation principle. Further, CBP has published a Privacy Impact Assessment for TVS that includes information on privacy protections, has a website for the program, and provides on-site signage to notify travelers about facial recognition, which relate to the transparency principle.

While CBP uses a variety of methods to provide privacy notices to travelers about the Biometric Entry-Exit Program and the use of facial recognition for traveler identification, in September 2020 we found that CBP's privacy notices to inform the public were not always current or complete, provided limited information on how to request to opt out of facial recognition, and were not always available. In particular,

[12] The Fair Information Practice Principles adopted by the DHS chief privacy officer are the basis for DHS's privacy policy and include the following 8 principles: Transparency, purpose specification, individual participation, data minimization, use limitation, security, data quality and integrity, and accountability and auditing. DHS requires its components—including CBP—to comply with the principles when using personally identifiable information. See Department of Homeland Security, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security,* DHS Privacy Policy Guidance Memorandum 2008–01; and *Privacy Policy and Compliance,* DHS Directive 047–01–001 (Washington, DC: July 25, 2011).

we identified limitations related to the completeness of information in CBP's on-line resources and call center, outdated signs at airports, information on opting out included in privacy notices, and placement of signs at ports of entry. For example:

- CBP on-line resources and call center had incomplete information. We found that CBP's public website on the Biometric Entry-Exit Program did not accurately reflect the locations where CBP used or tested FRT. Therefore, travelers who checked the website would not see a complete list of locations where they may encounter FRT. In addition, CBP has a call center for travel or customs questions. During five calls we placed to the call center between November 1, 2019, and January 1, 2020, we found the phone line was either not working or the operator was not aware of the ports of entry where facial recognition was in use or being tested.
- Signs at airports contained outdated information. We found that some signs at air exit locations (airport gates where facial recognition is used for departing travelers) were outdated, while others contained current information. For example, during our visit to the Las Vegas McCarran International Airport in September 2019, we saw one sign that said photos of U.S. citizens would be held for up to 14 days, and a second sign at a different gate that said photos would be held for up to 12 hours (the correct information). The first sign was an outdated notice, as CBP changed the data retention period for photos of U.S. citizens in July 2018. However, CBP had not replaced all of the signs at this airport with this new information. CBP officials said that they try to update signs when new guidance is issued but said that printing new signs is costly and it is not practical to print and deploy a complete set of new signs immediately after each change or update.
- Notices provided limited information on opting out of facial recognition identity verification. While CBP allows eligible travelers to request to opt out of facial recognition identity verification, the CBP notices we observed provided limited information on the process for opting out. For example, CBP's signs at airport facial recognition locations state that travelers who do not want to have their photos taken should see a CBP officer or a gate agent to "request alternative procedures for identity verification." However, the signs do not state what those alternatives are or the consequences of making such requests. In addition, CBP officers are typically not present at airport gates, so including this information on a sign could potentially be confusing to a traveler or make it less likely they would request to opt out during air exit.
- Signs were missing. We found that CBP signs at facial recognition locations were not consistently posted or were posted in such a way that they were not easily seen by travelers. CBP requires that its commercial partners—such as airlines, airports, or cruise lines—post CBP-approved privacy signs at gates where FRT is used to provide travelers with notice that their photos are being taken and for what purposes.[13] However, CBP has not enforced the requirement to post these signs or consistently monitored air exit facial recognition locations to ensure that signs are posted for each flight using FRT. For example, during our visit to the Las Vegas McCarran International Airport in September 2019, no privacy signs were posted at a gate where facial recognition had been in operation for about 2 months.

  CBP program officials noted that they have a relatively small office and they do not have the capacity to install signs for all new locations themselves or to conduct inspections to ensure that signs are present and visible. Instead, program officials said they rely on local CBP officers at airports to ensure that signs are posted in the appropriate locations through periodic checks. However, local CBP officers told us they do not have the personnel to check if signs are present at boarding gates for each flight that uses FRT since they have other duties and responsibilities and are not required by CBP policy or guidelines to do so. Nonetheless, CBP officials acknowledged that CBP is ultimately responsible for informing travelers about FRT across all environments and locations through signs, handouts, and the CBP website, among other methods.

[13] CBP allows commercial partners to use their own signs to provide notice of facial recognition, but these signs must be approved by CBP. CBP's requirements for commercial partners specify the minimum size for the signs, and specifies that the signs "must be clearly visible and placed at a sufficient distance in front of the camera in order to provide the traveler with a reasonable opportunity to read the content and opt-out before reaching the photo capture area." CBP also allows partners to display e-signage announcing the use of FRT. CBP's commercial partners may also choose to provide additional notices. For example, one airline official told us that their airline informs travelers about the use of FRT through emails sent along with reservation information.

In September 2020, we recommended that CBP ensure that the Biometric Entry-Exit Program's privacy notices contain complete and current information, including all of the locations where facial recognition is used and how travelers can request to opt out as appropriate. CBP implemented this recommendation. Specifically, CBP created a new website that outlines the locations (air, land, and sea ports) where CBP uses FRT. CBP also updated its biometrics website to include information on how travelers can opt out of the facial recognition verification process. Furthermore, CBP has begun providing its call center and information center staff with additional training, so staff are prepared to provide the public with complete and current information about the facial recognition verification program.

We also recommended that CBP ensure that the Biometric Entry-Exit Program's privacy signage is consistently available at all locations where CBP is using facial recognition. In June 2022, CBP reported that the program office developed a plan to ensure privacy signage for the Biometric Entry-Exit program is consistently available at all locations where FRT is used. As part of that plan, CBP officials said they reviewed the signage language and updated it to be more understandable by, for example, making it clearer that travelers can request alternative screening procedures. CBP also stated that the program office is in the process of upgrading the signs and intends to do so by September 2022. These actions, if fully implemented, should address the intent of our recommendation.

CBP Has Not Audited Most of Its Partners and Has Not Developed a Plan for Future Audits

CBP requires its commercial partners, as well as contractors and vendors, to follow CBP's data collection and privacy requirements, such as restrictions on retaining or using traveler photos, and CBP can conduct audits to assess compliance. However, in September 2020 we reported that as of May 2020, CBP had audited one of its more than 20 commercial airline partners and did not have a plan to ensure that all partners are audited for compliance with the program's privacy requirements. In particular, we found that although CBP's commercial airline partners have used FRT for identity verification since 2017, and cruise lines since 2018, CBP's first audit of a commercial partner occurred in March 2020. For this initial audit, CBP officials said they reviewed one commercial air carrier's privacy and security controls to ensure its compliance with program requirements. At that time, CBP officials said that they expected this initial audit to inform how they design and conduct future audits of commercial partners. However, CBP had not developed a plan with time frames for conducting audits of all of its commercial partners.

Similar to CBP's commercial partners, contractors and vendors associated with the Biometric-Entry Exit Program are subject to CBP's privacy and security requirements, including restrictions on their use of photos collected as part of the program, and CBP can audit them to ensure compliance. However, prior to a 2019 data breach involving a CBP subcontractor, CBP had not conducted security or privacy audits of its contractors. In 2019, a CBP subcontractor downloaded photos used in facial matching pilot testing at a land port of entry against CBP protocols.

The subcontractor was later the subject of a data breach.[14] CBP information security officials stated that it is unclear if this particular security vulnerability would have been identified through an audit because protocols were in place that prohibited contractors from downloading and removing data. However, after CBP identified this vulnerability, CBP information security officials began conducting security audits at some facial recognition testing locations to determine and assess security vulnerabilities. CBP officials also told us that they have made changes to pilot-testing security protocols, such as prohibiting the use of thumb (flash or USB) drives or any other personal drives. However, in September 2020, we reported that CBP

[14] According to CBP, a subcontractor employee involved with the pilot test at the Anzalduas land port of entry removed facial image data from the pilot site and then downloaded them to the company's network for the purpose of performing additional analysis of CBP's data. Data from the subcontractor's network was then stolen and posted on the dark web. CBP reviewed the dark web data and found no evidence that it included images from Anzalduas. CBP also confirmed that the subcontractor had only removed images; it did not have any associated data, such as names, dates of birth, or Social Security numbers. Officials said that they view this incident as an "insider threat" situation because the data were removed from CBP's systems in a way that was not authorized by policy or by contract. Officials also noted that the agency has a long-standing relationship with the prime contractor, and the subcontractor was vetted and screened by CBP. CBP officials told us that CBP immediately removed the subcontractor's access to CBP's systems after learning of the breach and asked the prime contractor to end the contract with the subcontractor. CBP has subsequently entered into an Administrative Contract Agreement with the subcontractor to improve their security practices but has no plans to resume business with the subcontractor.

did not have a plan to determine when all contractors and vendors would be audited for compliance with privacy and security requirements.

The Fair Information Practice Principles adopted by DHS state that agencies should audit the actual use of personal information to demonstrate compliance with all applicable privacy protection requirements. CBP officials acknowledged the importance of such audits but said they have generally not been a priority because CBP's contractors and partners do not have access to internal CBP databases and, therefore, cannot access systems that store personally identifiable information. CBP officials noted that, per CBP's requirements, partners agree they are not permitted to store or use photos obtained from the program in any way. When we spoke to representatives from the airline industry, they said that partner airlines and airports do not want to retain photos of travelers due to the risks and liability involved. However, as of May 2020, CBP had not yet audited the majority of its airline business partners to ensure they are adhering to CBP's privacy requirements.

In addition, while CBP had audited one of its airline partners and some locations where it was pilot-testing FRT, we reported that the privacy risks associated with personally identifiable information would continue to grow as the Biometric Entry-Exit Program expands and CBP collaborates with additional airlines, airports, cruise lines, contractors, and others. Thus, we recommended that CBP direct the Biometric Entry-Exit program to develop and implement a plan to conduct privacy audits of its commercial partners', contractors', and vendors' use of personally identifiable information. CBP concurred with our recommendation and, as of July 2022, officials said that CBP has conducted five assessments of its commercial partners in the air environment to ensure that they are adhering to CBP's requirements to protect travelers' privacy. Officials also said that three additional assessments are under way and that CBP has plans to assess about four partners in the air environment each year through 2025. These are positive steps to help ensure travelers' privacy is protected. To fully address the intent of our recommendation, CBP should complete its planned and in-progress assessments in the air environment. In addition, CBP should audit partners in the land and sea environments as well as vendors and contractors who have access to personally identifiable information.

CBP FOUND ITS AIR EXIT FACIAL RECOGNITION CAPABILITY MET ACCURACY REQUIREMENTS, BUT CBP HAS NOT FULLY MONITORED PERFORMANCE

During Operational Testing, Air Exit Met Accuracy Requirements but Did Not Meet Photo Capture Performance Requirement

As we reported in September 2020, air exit was the first Biometric Entry-Exit Program capability to progress through the DHS acquisition process and undergo formal operational testing and evaluation. As a DHS major acquisition program, consistent with DHS acquisition policy, the Biometric Entry-Exit Program's air exit facial recognition capability was to be assessed against program requirements in an operationally realistic environment before it could be fully deployed—referred to as operational testing.[15] From May to June 2019, an independent test agent within CBP performed an operational test and evaluation of air exit facial recognition capabilities.

CBP's operational testing determined that air exit met its defined accuracy requirements but did not meet one of its performance requirements. In its Operational Requirements Document for the Biometric Entry-Exit Program, CBP identified the capabilities needed to confirm the identities of travelers departing the United States by air, and included accuracy and performance requirements. In August 2019, the test agent found that air exit met or exceeded its two accuracy requirements. Specifically, the test found that air exit was able to correctly match 98 percent of travelers' photos with photo galleries built from passenger manifests, a key capability for the program. The test also found that air exit incorrectly matched a traveler to a gallery photo less than 0.1 percent of the time.

While air exit met its accuracy requirements during operational testing, it did not meet the program's photo capture performance requirement—that is, the percentage of in-scope travelers whose photos should be captured during the boarding process (also called the biometric compliance rate). Specifically, the test agent found that air exit successfully captured the photos of approximately 80 percent of in-scope

[15] A DHS major acquisition program is one with life cycle cost estimates of $300 million or greater. DHS policies for managing its major acquisition programs are primarily set forth in its Acquisition Management Directive 102.01 and Acquisition Management Instruction 102.01–001. For more information on DHS major acquisitions, see GAO, *Homeland Security Acquisitions: Outcomes Have Improved by Actions Needed to Enhance Oversight of Schedule Goals,* GAO–20–170SP (Washington, DC: Dec. 19, 2019).

travelers on participating flights, short of the 97 percent minimum requirement. According to the operational testing report, air exit did not meet the photo capture rate requirement due to disruptions to the facial recognition process during boarding. The report found that such disruptions were caused by factors such as camera outages, incorrectly configured systems at boarding gates, and airline agents' decisions to exclude certain categories of people, such as families or individuals using wheelchairs, to speed up the boarding process. In these cases, airline agents would revert to manual boarding procedures (i.e., visually comparing a traveler to his or her travel identification documents), and travelers' photos were not captured or transmitted to TVS. The test report noted that testing officials witnessed instances of cameras malfunctioning during boarding at all three of the airports they visited. During our observations of five flights at three airports in 2019, we identified similar photo capture issues with air exit.

To help air exit meet its performance requirement for capturing traveler photos, CBP's test agent recommended that the agency develop airline camera system standards to ensure they are capable of capturing photos of travelers of all heights, as well as investigate why partner airlines have issues with cameras during the boarding process. In response, CBP officials said they did not intend to take further action to improve the photo capture rate. Officials suggested that this was one metric of many used to assess the status of operational use of this capability. In addition, officials suggested that several factors would gradually improve the photo capture rate over time. These factors include a greater number of airline personnel trained on air exit facial recognition procedures and more efficient traveler interaction with cameras as familiarity with the facial recognition process increases (looking straight at the camera instead of down, for example). Because airline and airport partners participate in air exit voluntarily, they can choose to manually verify travelers' identities (not use FRT) for any reason. CBP officials said that air exit relies on these voluntary partnerships with airlines and airports, and they want to maintain positive relationships to recruit additional partners.

Air exit depends on the successful capture and submittal of live photos during boarding to fulfill its purpose of biometrically verifying traveler departures. At the time of our 2020 report, CBP did not intend to require airlines to capture photos of all in-scope travelers and did not have a plan to ensure that air exit could meet the 97 percent photo capture requirement defined in its operational requirements document. CBP officials stated that the photo capture rate would naturally improve as air exit expands throughout airports. However, we reported that improved familiarity with facial recognition procedures would not ensure that all applicable travelers are biometrically verified if partner airlines revert to manual identity verification, or if the photos they capture are low quality and cannot be matched.

In September 2020, we recommended that CBP develop and implement a plan to ensure that the biometric air exit capability meets its established photo capture requirement. CBP agreed with the recommendation. In June 2022, CBP officials noted that the photo capture rate requirement was included in the 2017 Operational Requirements Document when there was the possibility of CBP owning, operating, and maintaining cameras at airport departure gates. As the photo capture process was implemented, CBP determined that it does not have the staff to be present at every departure gate to oversee the process. Further, CBP does not require airlines to take a photo of every traveler. According to CBP officials, the photo capture requirement was removed from the latest draft of the Operational Requirements Document and CBP is waiting for the revised requirements to be fully approved by DHS, which it expected in August 2022. We will continue to follow up on the status of these revised requirements and the extent to which they may address our recommendation once approved by the department.

Effort to Assess the Accuracy of CBP's Facial Matching Across Demographic Variables

In addition to CBP's accuracy assessment conducted during the operational test of air exit capabilities, in December 2018, the National Institute of Standards and Technology (NIST)—a Government laboratory that has studied commercially available FRT—entered into an agreement with CBP to further assess the accuracy of TVS.[16] According to the terms of the agreement, NIST was to assess whether there

[16] While NIST has not set standards for how accurate a facial recognition system should be, NIST has conducted research into the accuracy of facial recognition algorithms since 2000. A NIST evaluation in December 2019 focused on testing the effects of demographics on matching accuracy of over 100 commercially-available facial recognition algorithms. NIST found that demographic effects in matching accuracy varied significantly across the algorithms it tested and

Continued

are differences in the accuracy of TVS based on traveler demographics such as age, gender, or ethnicity. According to CBP officials, CBP's internal analysis of data from air exit showed a negligible effect in matching accuracy based on demographic variables. However, officials noted that this analysis was limited because while CBP has access to data on age, gender, and nationality for travelers entering and exiting the country, it does not have data on race or ethnicity.

According to NIST officials, NIST intended to assess the accuracy of TVS by testing an algorithm similar to that used in TVS and analyzing the impacts of gender, ethnicity, and age on matching accuracy.[17] In September 2020, we reported that CBP planned to use the same matching algorithm for all travel environments, and NIST's findings on the demographic effects on matching accuracy planned to take into account all travel environments. Per the agreement, NIST was to provide technical information to CBP related to the algorithm, optimal thresholds, and gallery creation strategies.[18] NIST completed this report in July 2021.[19]

CBP's Process for Monitoring Air Exit Did Not Alert Officials When Performance Fell Below Minimum Requirements

In September 2020, we reported that CBP officials conduct monitoring of the accuracy and performance of air exit through random sampling, but the monitoring process did not alert them when performance fell below minimum requirements (such as the 97 percent photo capture rate described above). CBP officials said they randomly sampled two flights per airport per week and reviewed the data from each flight, including the number of matches and the match rate. Officials said that these reviews can help identify problems, such as unusually low match or photo capture rates, and they would investigate any identified problems by contacting the airline or airport where they occurred. In addition to random sampling, airline or airport officials can report problems with air exit facial recognition to CBP officials. CBP officials also noted that they generate automated reports of matching rates and usage on a weekly basis, and provide weekly performance reports to stakeholders, such as airline partners. Officials said they use this reporting to gauge system performance.

However, we reported that CBP's monitoring process did not immediately alert officials to problems that affect the performance of air exit. For example, randomly sampling flights for review on a weekly basis may not identify a daily pattern of consistently low-quality photos due to poor lighting in a particular terminal or airport. This means a problem at a particular terminal or airport could potentially continue unabated for days or even weeks, for example, without CBP's knowledge. CBP officials said there were several reasons why they chose random sampling to monitor the accuracy and performance of air exit. For example, officials said they had a small team of five analysts dedicated to monitoring air exit's performance, and they did not have the capacity or resources to manually review every flight for anomalies. Additionally, officials said air exit has returned consistently high match rates for photos that are successfully captured, which gave them confidence that more robust or comprehensive monitoring was not necessary.

However, CBP officials agreed it would be helpful if they had automatic alerts or notification when the performance for a flight or airport fell below air exit performance thresholds and acknowledged that their system has the capability to provide these automatic alerts. We recommended that CBP develop a process by which Biometric Entry-Exit program officials are alerted when the performance of air exit facial recognition falls below established thresholds. DHS agreed with our recommendation. In April 2021, CBP reported that it had developed various monitoring systems for the air exit facial recognition program. For example, CBP produces reports that provide program stakeholders with operational performance data by flight number, passenger counts, and biometric match rates. According to CBP, the program team monitors these reports for performance issues and addresses any anoma-

that many facial recognition systems performed differently among demographic groups. While NIST did not evaluate TVS, it included a version of the algorithm CBP uses with TVS in its evaluation and found it was among the most accurate algorithms on many measures. National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,* NISTIR 8280 (Dec. 2019).

[17] According to CBP officials, NIST was using CBP-owned photos from DHS databases, as well as photos from other sources, such as the Department of State and U.S. Citizenship and Immigration Services, to conduct its analysis.

[18] According to NIST, it intended to provide recommendations in the form of technical information that CBP can use to make informed decisions about its use of facial recognition algorithms.

[19] National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 7: Identification for Paperless Travel and Immigration,* NISTIR 8381 (July 2021).

lies with stakeholders as they arise. The program team also conducts random sampling to determine the technical match rates and to identify any system or equipment issues. Finally, the program team receives notifications if the system experiences an outage and has a gallery assembly system monitor that provides notifications when a flight gallery is not created. These actions addressed the intent of our recommendation.

Chairwoman Barragán, Ranking Member Higgins, and Members of the subcommittee, this completes my prepared statement. I would be happy to respond to any questions you or the Members of the subcommittee may have.

Chairwoman BARRAGÁN. Thank you for your testimony. I will now recognize Mr. Jeramie Scott to summarize his statement for 5 minutes.

STATEMENT OF JERAMIE D. SCOTT, SENIOR COUNSEL, ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

Mr. SCOTT. Thank you, Chairman Barragán, Ranking Member Higgins, and Members of the subcommittee. Thank you for holding this hearing and for the opportunity to testify today on CBP use of facial recognition technology.

My name is Jeramie Scott, senior counsel of the Electronic Privacy Information Center, or simply EPIC. EPIC is an independent nonprofit research organization in Washington, DC, established in 1994 to protect privacy, freedom of expression, and the democratic values in the information age.

Facial recognition is dangerous surveillance technology because the risks increase as the Government expands its implementations in any form, including for identity verification. The technology poses serious threats to our privacy, our civil liberties, our Constitutionally-protected rights, and our democracy. Facial recognition has accuracy and bias issues that are most likely to impact marginalized groups, but even a perfectly accurate and unbiased facial recognition system poses fundamental risks to a democratic society when widely deployed. CBP has implemented one of the most widely deployed facial recognition systems in the country with its Biometric Entry-Exit Program.

The program uses facial recognition to verify the identity of travelers entering and exiting the United States. Facial recognition is applied to all travelers, including U.S. citizens, despite Congress never granting CBP authority to conduct facial recognition verification on U.S. citizens.

Nonetheless, CBP has forged ahead by obtaining passport photos from the State Department to use for facial recognition at international airports and other ports of entry. Although U.S. citizens can, in theory, opt out of facial recognition, this hasn't been easy to do in practice. The Government Accountability Office, as we just heard, and a DHS Data Privacy and Integrity Advisory Committee both found that CBP failed to provide adequate notice about the use of facial recognition at airports or information about the opt-out procedure.

Even if a U.S. citizen is able to opt out of facial recognition, there is no way for that person to opt out having their photo obtained by CBP from the State Department used as part of the facial recognition photo galleries created for the Biometric Entry-Exit Program.

This is particularly important given the data breach of the CBP subcontractor where 184,000 images of travelers from the Biometric Entry-Exit Program were exposed, images the subcontractor was not supposed to have. But CBP's security and privacy protocols failed to prevent the subcontractor from obtaining these images.

CBP's track record for not properly administering the Biometric Entry-Exit Program does not provide comfort as the agency seeks to continue to expand the program. History tells us that if the program continues its expansion unchecked, it will not just expand in the number of the ports the program it is implemented at, but in the number of situations CBP's facial recognition system is used for. CBP has described the future airport process as one where every step from dropping off baggage, moving through TSA checkpoints, and boarding planes is mediated by facial recognition scans.

The on-going expansion of CBP's facial recognition system creates a powerful and dangerous tool of surveillance for the Federal Government. CBP has access to millions of passport and visa photos held by the State Department in addition to the millions of photos the Department of Homeland Security holds in its biometric database. The facial recognition system CBP has built is a cloud-based system that can easily be connected to additional sources of photos.

The unfettered use of facial recognition to verify identity puts us on a path toward a ubiquitous universal ID controlled by the Government. Unless regulations are put in place to end or at least limit the Biometric Entry-Exit's use of facial recognition technology the program will continue to expand well beyond its intended purpose.

The safest investment would be for CBP to end its use of facial recognition technology. This would eliminate the risk of CBP's facial recognition technology infrastructure being used for more pervasive surveillance as a ubiquitous identification system.

At minimum, Congress should put in place the following requirements for CBP's use of facial recognition technology. A requirement to use a one-to-one facial recognition system that does not require a database or connection to the cloud. A prohibition on the use of facial recognition services provided by third parties, like Clearview AI. A prohibition on any law enforcement agency using CBP's facial recognition system for generalized investigative leads. A requirement that CBP only use its facial recognition system for identity verification as part of the Biometric Entry-Exit Program. And a requirement for annual audits for CBP's facial recognition system conducted by an independent third party.

If the Biometric Entry-Exit Program is to remain in operation, these safeguards are critical to protect privacy, civil liberties, civil rights, and the security of sensitive biometric data.

Thank you for the opportunity to testify today. I would be happen to answer any questions.

[The prepared statement of Mr. Scott follows:]

PREPARED STATEMENT OF JERAMIE D. SCOTT

JULY 27, 2022

Chairwoman Barragán, Ranking Member Higgins, and Members of the subcommittee, thank you for holding this hearing and for the opportunity to testify today on CBP's use of facial recognition technology. My name is Jeramie Scott, senior counsel at the Electronic Privacy Information Center, or simply EPIC. EPIC is an independent nonprofit research organization in Washington, DC, established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.

EPIC has long history of work on facial recognition and the privacy and civil liberties issues the technology raises, particularly with respect to Custom and Border Protection's (CBP's) use of facial recognition.[1] The attention is warranted and necessary because facial recognition is a dangerous surveillance technology whose risks increase as the Government expands its implementations in any form, including for identity verification. The technology poses serious threats to our privacy, our civil liberties, our Constitutionally-protected rights, and our democracy. Facial recognition has accuracy and bias issues that are most likely to impact marginalized groups. But, even a perfectly accurate and unbiased facial recognition system poses fundamental risks to a democratic society when widely deployed.

In my testimony I will discuss the issues with facial recognition in general, CBP's use of facial recognition as part of its Biometric Entry-Exit program, the many issues with this program, and the threat CBP's use of facial recognition poses to individuals and our society.

I. FACIAL RECOGNITION TECHNOLOGY IS INACCURATE AND BIASED

Facial recognition systems have been deployed by both Government agencies and private companies with little to no oversight, despite many questions regarding their effectiveness.[2] A 2019 National Institute of Standards and Technology ("NIST") study of facial recognition tools—which are typically "AI-based"[3]—found that the systems were up to 100 times more likely to return a false positive for a non-white person than for a white person.[4] Specifically, NIST found that "for one-to-many matching, the team saw higher rates of false positives for African American females," a finding that is "particularly important because the consequences could include false accusations."[5] A separate study by Stanford University and MIT, which looked at three widely-deployed commercial facial recognition tools, found an error rate of 34.7 percent for dark-skinned women compared to an error rate of 0.8 percent for light-skinned men.[6] A review of Rekognition—an Amazon-owned facial recognition system marketed to law enforcement—revealed indications of racial bias

[1] See e.g., Comments of EPIC to U.S. Customs and Border Protection Dept., Collection of Advance Information From Certain Undocumented Individuals on the Land Border, Docket ID: USCBP–2021–0038 (Nov. 29, 2021), *https://epic.org/wp-content/uploads/2021/11/EPIC-Comments-DHS-Advance-Collection-Photos-Border-Nov-2021.pdf,* Comments of EPIC to the Transportation Security Admin., Intent to Request Revision of Agency Information Collection Activity Under OMB Review: TSA PreCheck, Docket ID: TSA–2013–0001 (June 22, 2020), *https://epic.org/apa/comments/EPIC-TSA-PreCheck-FRT-Comment-June2020.pdf;* Comments of EPIC to the Dept. of Homeland Security, Agency Information Collection Activities: Biometric Identity, Docket No. 1651–0138 (Jul. 24, 2018), *https://epic.org/apa/comments/EPIC-CBP-Vehicular-Biometric-Entry-Exit-Program.pdf; EPIC* v. *CBP (Biometric Entry/Exit Program), https://epic.org/foia/dhs/cbp/biometric-entry-exit/default.html* (EPIC obtained a report which evaluated iris imaging and facial recognition scans for border control); EPIC Statement to U.S. House Comm. on Homeland Security, "Border Security, Commerce and Travel: Commissioner McAleenan's Vision for the Future of CBP" (Apr. 24, 2018), *https://epic.org/testimony/congress/EPIC-HHSC-CBP-Apr2018.pdf;* Comments of EPIC to the Dept. of Homeland Security, Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Citizenship and Immigration Services—018 Immigration Biometric and Background Check (IBBC) System of Records, Docket Nos. DHS–2018–0002 and DHS–2018–0003 (Aug. 30, 2018), *https://epic.org/apa/comments/EPIC-DHS-Immigration-Biometric-Database.pdf;* Comments of EPIC to the Dept. of Homeland Security, Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States (Dec. 21, 2020), *https://epic.org/documents/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states/.*

[2] David Freeman Engstrom, Daniel E. Ho, Catherine M. Sharkey, & Mariano-Florentino Cuéllar, *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies* 6 (Feb. 2020), *https://www-cdn.law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf.*

[3] Nat'l Inst. Standards & Tech., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* 14 (Dec. 2019), *https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.*

[4] Nat'l Inst. Standards & Tech., *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software* (Dec. 19, 2019), *https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.*

[5] Id.

[6] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* Proceedings of Machine Learning Research 81:1–15 (2018), *https://www.media.mit.edu/publications/gender-shades-intersectional-accuracy-disparities-in-commercial-gender-classification/.*

and found that the system misidentified 28 members of U.S. Congress as convicted criminals.[7] Yet CBP is relying on this flawed technology to protect our borders.

II. CBP'S BIOMETRIC ENTRY-EXIT PROGRAM

CBP has implemented one of the largest deployments of facial recognition technology in the country through its Biometric Entry-Exit program. According to CBP, 238 airports use facial recognition for entry and 32 airports have facial recognition deployed for exit.[8] Another 13 seaports use facial recognition and almost all the processing facilities for pedestrians and buses along the Northern and Southern Border deploy facial recognition.[9] And since 2017, CBP has used facial recognition on over 100 million travelers.[10] Further, the agency has "the ultimate goal of implementing a comprehensive biometric entry-exit system Nation-wide".[11]

The backbone of CBP's Biometric Entry-Exit program is the agency's Traveler Verification Service (TVS). TVS is a cloud-based information technology that handles the actual facial recognition comparison.[12] TVS uses biometric templates created from existing photographs obtained from several sources including U.S. passport and U.S. visa photos from the State Department, images captured during entry inspection, and other encounters with the Department of Homeland Security where a photograph is taken.

CBP leverages these photographs to build specific galleries of photographs for entry and exit points.[13] For example, for commercial flights, where CBP knows ahead of time who will be on a given flight, the agency builds a gallery of photos based on expected passengers. At the borders where people may be crossing on foot or in their own vehicles, "CBP will build galleries using photographs of "frequent" crossers for that specific port of entry, taken at that specific port of entry, that become part of a localized photographic gallery."[14] These photo galleries are used by TVS to create the face prints or biometric templates used for facial recognition identification.[15] Where CBP has implemented the Biometric Entry-Exit program, the agency applies facial recognition identification to all travelers, including U.S. citizens.[16] The implementation of the Biometric Entry-Exit program has been a slow and long process—one fraught with issues in the program's administration, lack of clear rationale, and questionable authority. Despite the issues, CBP submitted a Notice of Proposed Rulemaking in November 2020 to make permanent the agency's implementation of a biometric entry-exit system that utilizes facial recognition identification. The CBP's efforts to expand the use of facial recognition through the Biometric Entry-Exit program lacks the necessary authority to collect biometrics on U.S. citizens, unnecessarily expands the program beyond its apparent purpose, and creates an unregulated facial recognition infrastructure likely to be exploited by the Government in the future.

III. CONGRESS NEVER GAVE CBP THE LEGAL AUTHORIZATION TO COLLECT BIOMETRIC DATA FROM U.S. CITIZENS

CBP lacks the legal authorization to collect biometric data from U.S. citizens. As part of its implementation of "an integrated automated entry and exit data system . . . of aliens entering and departing the United States," CBP has proposed collecting not only biometric information from noncitizens crossing the U.S. border, but also biometric information from U.S. citizens.[17] In support of its decision to col-

[7] Russell Brandom, *Amazon's facial recognition matched 28 Members of Congress to criminal mugshots,* The Verge (July 26, 2018), *https://www.theverge.com/2018/7/26/17615634/amazon-rekognition-aclu-mug-shot-congress-facial-recognition.*

[8] CBP, *Introducing Biometric Facial Comparison, https://biometrics.cbp.gov.*

[9] Id.

[10] CBP, *Introducing Biometric Facial Comparison, https://biometrics.cbp.gov.*

[11] Notice of proposed rulemaking on "Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States," 85 Fed. Reg. 74162, 74163 (Nov. 19, 2020), *https://www.govinfo.gov/content/pkg/FR-2020-11-19/pdf/2020-24707.pdf.*

[12] DHS, *Privacy Impact Assessment for the Traveler Verification Service 4–6* (Nov. 14, 2018), *https://www.dhs.gov/sites/default/files/publications/PIA%20for%20Traveler%20Verification-%20Service.pdf* (hereinafter ("PIA".)

[13] Id. at 5.

[14] Id. at 5.

[15] Id. at 6.

[16] U.S. citizens are able to opt-out of facial recognition identification but as described below the opt-out is not meaningful and has not always been honored by CBP agents.

[17] Collection of Biometric Data from Aliens upon Entry to and Departure from the United States, 85 Fed. Reg. 74,162 (Nov. 19, 2020); see also Collection of Biometric Data from Aliens upon Entry to and Departure from the United States; Re-Opening of Comment Period, 86 Fed. Reg. 8,878 (Feb. 10, 2021).

lect this information, CBP reports that it had identified several "imposters" who had attempted to enter the United States using U.S. travel documents that did not belong to them.[18] In addition, CBP justifies the collection of biometric information from U.S. citizens by stating that photos of U.S. citizens used for face verification would only be stored for 12 hours after confirmation of a person's identity.[19]

CBP's justifications for collecting biometric information from U.S. citizens are insufficient, however, as Congress has only authorized CBP to deploy a biometric entry/exit program for noncitizens. Evidence that Congress limited its authorizations to noncitizens is found in numerous prior statutes establishing an entry/exit system—some of which are cited by CBP itself in its notice of proposed rulemaking, and none of which mention U.S. citizens. As authority for its proposed rule to collect the biometric data, CBP relies on the 2016 Consolidated Appropriations Act.[20] In that statute, Congress instructed the DHS Secretary to submit to Congress a plan to "implement[] . . . the biometric entry and exit data system described in section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004" and allocated funding toward that implementation.[21]

Context and statutory language make it clear that Congress never intended to authorize CBP to collect biometric information from citizens. For one, the Intelligence Reform and Terrorism Prevention Act referenced in the 2016 Appropriations Act applies only to noncitizens. The statute authorized collecting biometric exit data for "all categories of individuals who are required to provide biometric entry data, regardless of the port of entry where such categories of individuals entered the United States."[22] After this authorization, the subsequent section of the Act grants the DHS Secretary with the authority "to integrate all databases and data systems that process or contain information on aliens . . . "[23]

Moreover, all existing statutes that identify categories of people "required to provide biometric entry data" apply only to noncitizens.[24] These statutes include the "Illegal Immigration Reform and Immigrant Responsibility Act of 1996," in which Congress authorized collection of biometrics at the border from noncitizens crossing the U.S. border.[25] It also includes a statute passed in 2007, which required DHS to "establish an exit system" that includes biometric collection for "every alien participating in the visa waiver program."[26] In fact, none of the entry-exit system statutes that CBP cites to justify its proposed rule mention U.S. citizens.[27]

[18] 85 Fed. Reg. at 74, 167.

[19] Id. at 164.

[20] Id. at 74, 164–65.

[21] Pub. L. 114–113, 129 Stat. 2242, 2493, 3006 (2015).

[22] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458, § 7208(d) (2004).

[23] Id. at § 7208(e) (emphasis added).

[24] See Harrison Rudolph et al., Not Ready for Takeoff: Face Scans at Airport Departure Gates, Geo. Ctr. on Privacy & Tech 7 (2017).

[25] H.R. Rep. No. 104–828 (1996) § 104 (amending 8 U.S.C. 1101(a)(6)); see also 8 U.S.C. 1101(a)(6).

[26] Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110–53, § 711(i)(1)–(2), 121 Stat. 266, 345 (2007).

[27] In its November 2020 notice of proposed rulemaking, Collection of Biometric Data from Aliens upon Entry to and Departure from the United States, 85 Fed. Reg. 74,162, 74,165 (Nov. 19, 2020), CBP cites to the following statutory authorities "requir[ing] DHS to take action to create an integrated entry-exit system." Each of these statutes—except for the last statute, which is the general statute establishing the CBP agency—do not mention U.S. citizens in relation to their discussion of the entry/exit system:

- Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law 104–828, 110 Stat. 3009–546 (authorizing collection of biometric identification from noncitizens crossing the U.S. border);
- Section 205 of the Visa Waiver Permanent Program Act of 2000, Public Law 106–396, 114 Stat. 1637, 1641 (calling for the implementation of "a fully automated entry and exit control system that will collect a record of arrival and departure for every alien" under the visa waiver program (emphasis added);
- Section 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Public Law 107–56, 115 Stat. 272, 353 (instructing the Executive branch to "expedite" implementation of the entry/exit data system specified in the Illegal Immigration Reform and Immigrant Responsibility Act of 1996);
- Section 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), Public Law 107–173, 116 Stat. 543, 552 (requiring Federal officials to "establish a database containing the arrival and departure data from machine-readable visas, passports, and other travel and entry documents possessed by aliens" (emphasis added));
- Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110–53, 121 Stat. 266, 338 (concerning "modernization of the visa waiver program");

Continued

IV. CBP HAS FAILED FROM THE BEGINNING OF PROGRAM TO PROVIDE A REASONABLE JUSTIFICATION FOR THE EXPANSION OF THE BIOMETRIC EXIT PROGRAM

From the start, CBP's justifications for implementing the Biometric Exit system have changed and expanded. Recording biometric data from non-citizens leaving the United States was briefly mentioned as a recommendation of the 9/11 Commission.[28] The 9/11 Commission only discussed the possibility of biometric border screening in passing and did not explain how such a system could meaningfully improve National security.

In the years after the 9/11 Commission Report, DHS moved slowly to implement a biometric exit system, in part because DHS components could identify no rationale for the program. In 2012, an internal DHS Science and Technology Directorate evaluation found that "significant questions remained" on "(3) the additional value biometric air exit would provide compared with the current biographic air exit process, and (4) the overall value and cost of a biometric air exit capability."[29] After responsibility for Biometric Exit was assigned to CBP in 2013, the agency settled on a rationale of using the program to prevent visa overstays, but at the time there was no evidence that collecting biometrics on departure from the United States would address this problem.[30] CBP has since been able to quantify the effectiveness of using only biographic identifiers for non-citizens exiting the United States, stating that collecting biographic information is "accurate for approximately 98–99 percent of foreign travelers who entered under a visa (or the visa waiver program)."[31]

Although CBP has forged ahead in implementing Biometric Exit, agency analysts are skeptical of the value of the program to this day. In 2017, a senior DHS official could not tell the DHS Data Privacy and Integrity Advisory Committee how Biometric Exit would improve the immigration system and claimed vague "immigration and counterterrorism benefits."[32] But CBP has repeatedly disclaimed any possible counterterrorism benefits of Biometric Exit.[33] A 2020 report from the Homeland Security Advisory Committee described biographic data collection as sufficient for visa overstay enforcement and objected that, "even if a marginal case could be made for biometric exit, it has never been evaluated on a cost-benefit basis."[34] However, CBP's response to this long-standing and cogent analysis makes little sense. In the face of purported difficulties with separating out U.S. citizens from Biometric Exit, the agency threw up its hands and claimed that imposing facial recognition on both citizens and non-citizens was the only solution.[35]

• Section 802 of the Trade Facilitation and Trade Enforcement Act of 2015, Public Law 114–125, 130 Stat. 122, 199 (6 U.S.C. 211(c)(10)) (establishing CBP).

[28] National Commission on Terrorist Attacks upon the U.S., The 9/11 Commission Report 387–390 (July 22, 2004), available at *https://www.9-11commission.gov/report/911Report.pdf* (hereinafter "9/11 Commission Report").

[29] As summarized in U.S. Government Accountability Office, GAO–16–358T, Actions Needed by DHS to Address Long-Standing Challenges in Planning for a Biometric Exit System: Before the Subcommittee on Immigration and the Nat'l Interest, Committee on the Judiciary, U.S. Senate, 115th Cong. 8 (Jan. 20, 2016) (Statement of Rebecca Gambler, Director Homeland Sec. and Justice), *https://www.gao.gov/assets/680/674704.pdf.*

[30] See Written testimony of U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement for a House Committee on Homeland Security, Subcommittee on Border and Maritime Security hearing titled "Fulfilling A Key 9/11 Commission Recommendation: Implementing Biometric Exit" (Sept. 23, 2013), *https://www.dhs.gov/news/2013/09/26/written-testimony-cbp-and-ice-house-homeland-security-subcommittee-border-and.*

[31] Homeland Security Advisory Council (HSAC), Subcommittee on Biometrics, Final Report of the Biometrics Subcommittee at 30 (Nov. 12, 2020), *https://www.dhs.gov/sites/default/files/publications/final__hsac__biometrics__subcommittee__report__11-12-2020.pdf.*

[32] U.S. Department of Homeland Security, DPIAC Meeting Minutes 5 (Sept. 19, 2017), *https://www.dhs.gov/sites/default/files/publications/DPIAC%20Meeting%20Minutes-Sept%2019%202017.pdf* ("Q(LG): does this solve your problem with overstaying/terrorism? A(MH): not our role to question duly passed laws from Congress. We think it gives us immigration and counterterrorism benefits. We trust in Congress and 9/11 Commission.").

[33] Homeland Security Advisory Council (HSAC), Subcommittee on Biometrics, Final Report of the Biometrics Subcommittee at 30 (Nov. 12, 2020), *https://www.dhs.gov/sites/default/files/publications/final__hsac__biometrics__subcommittee__report__11-12-2020.pdf* ("Unlike biometric entry, biometric exit has little to do with preventing terrorist attacks." and "Neither CBP nor DHS has ever assessed that a biometric exit capability is needed for National security or counter-terrorism purposes.").

[34] Id.

[35] Id. "In an effort to comply with Congressional mandates, CBP's choice to pursue facial recognition specifically, as opposed to any of the various other biometric modalities, was largely a consequence of an unavoidable reality."

V. CBP HAS FAILED TO PROPERLY ADMINISTER ITS BIOMETRIC ENTRY-EXIT PROGRAM

CBP's implementation of the Biometry Entry/Exit program has consistently fallen below baseline standards for privacy articulated in DHS's Fair Information Privacy Principles (FIPPs).[36] The FIPPs set benchmarks for data collection and use that DHS must meet to comply with the Privacy Act of 1974.[37] The FIPPs comprise eight mandates: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability/ Auditing.[38] By DHS policy, the FIPPs "must be considered whenever a DHS program or activity raises privacy concerns or involves the collection of personally identifiable information from individuals, regardless of their status."[39] If CBP cannot meet their own metrics for ensuring privacy when using facial recognition then the agency should not collect that data.

a. CBP failed to meet the FIPPs of Transparency and Individual Participation by not providing adequate notice of facial recognition programs

The Government Accountability Office (GAO) previously investigated CBP's Biometric Entry/Exit program.[40] In a September 2020 report, the GAO found four major shortcomings in CBP's Biometric Entry/Exit program. Together, these failures demonstrate that CBP is either unable or unwilling to take basic steps to protect individuals' privacy, often falling short of DHS's own FIPPs.

First, the GAO found that CBP routinely failed to provide adequate notice and opt out procedures. At the time of the GAO's investigation, CBP's on-line resources on facial recognition programs had incomplete information and did not list all of the locations where CBP had deployed facial recognition.[41] Similarly, CBP did not provide enough information for call center employees to answer questions about facial recognition.[42] The call center was often off-line, and when GAO could get through, operators did not know which air and land ports were using facial recognition.[43]

Second, signs at airports were consistently outdated and contradictory. The GAO found that signs within a single airport contained contradictory information on data retention policies.[44] CBP claimed their failure to update signage was justified by the prohibitive cost of printing signs.[45] CBP has not prioritized updating posted notices to reflect current procedures and data retention protocols. CBP appears unconcerned with providing accurate and meaningful notice to travelers.

Third, the GAO faulted CBP for providing inadequate information on how travelers could opt out of facial recognition identity verification.[46] CBP's signs mentioned an opt-out but did not describe what "alternative procedures" travelers would have to go through in lieu of facial recognition.[47] Throughout its implementation of Biometric Entry/Exit CBP has provided vague and inconsistent descriptions of alternative screening procedures. In 2018, EPIC obtained documents through a FOIA lawsuit revealing that CBP had developed a detailed opt-out and alternative screening procedure.[48] But the agency did not describe that procedure to the public.[49] This critique echoes the Data Privacy and Integrity Advisory Committee's report from 2019 which recommended basic improvements to CBP's written notices to improve readability, ensure adequate time for consideration, and explain opt-out proce-

[36] Hugo Teufel III, The Fair Information Practice Principles: Framework for Privacy Policy at the Dept. of Homeland Security Memorandum Number 2008–01, Dep't. of Homeland Sec. (Dec. 29, 2008), *https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.*

[37] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

[38] DHS FIPPs Memorandum, supra note 36, at 4.

[39] DHS FIPPs Memorandum, supra note 36.

[40] U.S. Gov't Accountability Off., GAO–20–568 *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues* (Sept. 2020) (hereinafter GAO Facial Recognition Report), *https://www.gao.gov/products/GAO-20-568.*

[41] Id. at 39.

[42] Id. At 39–40.

[43] Id.

[44] Id. at 40.

[45] Id.

[46] Id. at 41.

[47] Id.

[48] U.S. Customs and Border Prot., Traveler Verification Service: Standard Operating Procedure at 9 (June, 2017), *https://epic.org/foia/dhs/cbp/biometric-entry-exit-alt-screening-procedures/Traveler-Verification-Service-SOP-June2017.pdf;* U.S. Customs and Border Prot., Biometric Air Exit: Standard Operating Procedure (Mar. 2019), *https://epic.org/foia/dhs/cbp/biometric-entry-exit-alt-screening-procedures/Biometric-Air-Exit-SOP-Mar2019.pdf.*

[49] See *EPIC* v. *CBP* (Biometric Entry-Exit Alternative Screening Procedures), *https://epic.org/documents/epic-v-cbp-biometric-entry-exit-alternative-screening-procedures/.*

dures.[50] CBP has for years been on notice that the agency needs to provide and publicize a clear opt-out procedure, but the agency has failed to do so.

Fourth, CBP and its corporate partners routinely failed to post signs or obscured notices on facial recognition. The GAO observed that "facial recognition signs were not consistently posted or were posted in such a way that they were not easily seen by travelers."[51] Where CBP delegates responsibility for posting signs to commercial airlines, the GAO found that the agency did not enforce or monitor this requirement.[52] As a result, required signs are often missing. The GAO also observed signs that were difficult to read because they were posted far away from travelers and written in small print.[53] Facial recognition notices are also often blocked by other signs so that they could not be read.[54] CBP claims that their Biometric Entry/Exit staff is small, and cannot ensure signs are posted so they rely on local airport agents.[55] Yet CBP's airport agents told the GAO that they did not check signs, and were not required to do so.[56] CBP has historically been unable to ensure that travelers receive adequate, or often any, notice that they can opt out of one of the most invasive technologies in use today.

By not providing travelers meaningful notice and the time to consider their options, the GAO found that CBP has not met its requirements under the FIPPs of Transparency and Individual Participation.[57] While providing notice may not be the strongest step CBP can take to protect individuals' personally identifiable information, it is the easiest. If CBP cannot or will not take the basic steps necessary to provide travelers with adequate notice of facial recognition, then the agency's ability to provide more substantive protection is dubious at best.

CBP's failure to provide notice of its facial recognition policies has caused real privacy harms. The GAO received reports of incidents of individuals "being told by CBP officers and airline agents that opting out would lead to additional security scrutiny, increased wait times, and could be grounds to deny boarding."[58] Although CBP claims to provide opt-out procedures which do not inconvenience or prejudice travelers, the agency is clearly failing to adequately inform its employees and the general public of these procedures. At every turn, CBP has failed to adequately implement its opt-out procedures.

b. CBP has not performed necessary audits to ensure facial recognition images are secure

In its review, the GAO found that CBP "has not audited most of its partners and has not developed a plan for future audits."[59] CBP's agreements prohibit corporate partners from retaining images for their own purposes and require partners to expediently delete images, but CBP does not adequately ensure those contract terms are followed.[60] CBP has allowed its partners to use facial recognition technology for identification since 2017.[61] It took 3 years for the agency to perform its first audit of an airline.[62] As far as I am aware, the agency still has not audited a cruise line. In that time, over 7 million passengers have submitted to facial recognition by more than 20 airlines and cruise lines.[63] More than 95 percent of CBP's corporate partners have never received an audit. The agency has no idea if its partners are taking individuals' images for their own purposes or complying with data retention requirements.

The GAO's findings echo DPIAC's findings, in which the committee stressed that "it is important to ensure transparency in the process, strong contractual guidelines,

[50] DHS Data Privacy and Integrity Advisory Committee, Report 2019–01 of the DHS Data Privacy and Integrity Advisory Committee (DPIAC): Privacy Recommendations in Connection with the Use of Facial Recognition Technology at 4–5 (Feb. 26, 2019) (hereinafter DPIAC Facial Recognition Recommendations), *https://www.dhs.gov/sites/default/files/publications/-Report%202019-01__Use%20of%20Facial%20Recognition%20Technology__02%2026%202019.pdf.*

[51] GAO Facial Recognition Report at 42.

[52] Id.

[53] Id. at 44.

[54] Id.

[55] Id. at 43.

[56] Id.

[57] Id. at 46.

[58] GAO Facial Recognition Report at 42; see also Shaw Drake, *A Border Officer Told Me I Couldn't Opt Out of the Face Recognition Scan. They Were Wrong.,* ACLU (Dec. 5, 2019), *https://www.aclu.org/news/immigrants-rights/a-border-officer-told-me-i-couldnt-opt-out-of-the-face-recognition-scan-they-were-wrong/.*

[59] Id. at 46.

[60] Id.

[61] Id.

[62] Id.

[63] Id.

auditing, and rigor in the process of ensuring the FIPPs are adhered to."[64] The DPIAC called for thorough audits as a necessary step to protect particularly sensitive facial recognition images.[65] Yet despite the DPIAC's urgings, CBP has performed only one audit of its commercial partners and seemingly has no plan in place for further audits of either its commercial partners or its contractors. This amounts to willful blindness on the part of the agency. CBP's failure to perform necessary audits for years displays a callous disregard for individuals' privacy, even after the agency suffered a serious data breach of its facial recognition systems.

c. CBP has been unable to safeguard facial recognition images

Recent data breaches and hacks within CBP and across the Federal Government demonstrate that CBP is incapable of safeguarding sensitive personal information such as facial recognition images. In 2016 the U.S. Government Accountability Office warned that "[c]yber-based intrusions and attacks on Federal systems have become not only more numerous and diverse but also more damaging and disruptive."[66] The GAO called on DHS to enhance cybersecurity protection in key areas including intrusion detection and prevention. At the time DHS had not even put in place an adequate process for sharing information on intrusions and potential malicious activity.[67] Since that time DHS and its subcomponents have not shown that they are capable of adequately safeguarding personally identifiable information, particularly biometric data.

In 2019 a data breach at CBP subcontractor Perceptics, LLC exposed approximately 184,000 images of travelers from a CBP Biometric Entry/Exit pilot.[68] Perceptics staff were able to violate several DHS security and privacy protocols to download the images used for facial recognition without CBP's IT security controls preventing the unauthorized action or sounding an alarm.[69] When Perceptics, LLC was subsequently hacked, outside agents had access to those 184,000 images and an additional 105,000 license plate images.[70] At least 19 facial recognition images were released on the dark web.[71] DHS's Office of the Inspector General found that, "Perceptics was able to make unauthorized use of CBP's biometric data, in part because CBP did not implement all available IT security controls, including an acknowledged best practice."[72] OIG concluded that CBP "[d]id not adequately fulfill its responsibilities for IT security".[73]

Data breaches are common across the Federal Government—often exposing the PII of millions to exploitation and abuse. But data that is never collected in the first place is not at risk of breach. CBP should not unnecessarily collect sensitive personally identifiable information on millions of travelers when the agency cannot even protect the data it currently holds.

VI. THE EXPANSION OF CBP'S BIOMETRIC ENTRY-EXIT PROGRAM CREATES A POWERFUL AND DANGEROUS TOOL OF SURVEILLANCE FOR THE FEDERAL GOVERNMENT

Through the Biometric Entry-Exit program, CBP can access millions of photos of U.S. citizens through the State Department. Additionally, DHS retains millions of photos in its IDENT database that are accessible to CBP. As part of the Biometric Entry-Exit system, CBP has created a cloud-based facial recognition system that allows the agency to easily connect the system to its own cameras or the cameras of its partners to perform facial identification. One of the main reasons CBP chose to use facial recognition is that the images were easy to obtain and facial recognition technology is easy to apply to existing systems. The result is an expansion of an infrastructure that could easily be used for mass surveillance and/or a universal digital ID controlled by the Government.

[64] DPIAC Facial Recognition Report at 10.

[65] Id. at 10–12.

[66] U.S. Gov't Accountability Office, DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System (Jan. 2016), *https://www.gao.gov/assets/680/674829.pdf.*

[67] Id. at 27.

[68] Joseph Cuffari, Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot, Dep't of Homeland Sec. Off. of Inspector Gen. (Sept. 21, 2020), *https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.*

[69] Id. at 6.

[70] Id. at 8.

[71] Id. at 13.

[72] Id. at 12.

[73] Id.

a. CBP's Biometric Entry-Exit program creates a ubiquitous, universal ID controlled by the Government

The continued use of facial recognition identification through CBP's Biometric Entry-Exit program puts the United States on a path toward a ubiquitous and universal form of identification that will destroy anonymity and give the Government complete control over identification. No longer will an individual have any control over their identification and have choice when to identify themselves or not. A facial recognition identification system leveraging hundreds of millions of photos held by the Government will give CBP and other Government agencies the power to identify individuals whether or not that individual consents and regardless if the Government has legitimate grounds for wanting to identify the individual. And there will be little recourse.

Our face's geometry that is used to create the face prints for facial recognition is unique to each person and for the most part can't be changed. And unlike other forms of biometric recognition or identity verification, facial recognition can easily be applied covertly, from a distance, and without our consent or knowledge. Because our faces are generally exposed and photographs are required for Government identifications like passports, it is virtually impossible to insulate ourselves from facial recognition technology. Once the Government has a person's faceprint, it creates a unique risk of unprecedented and persistent surveillance—one that allows the Government to identify and track people without their knowledge.

b. Unless regulations are put in place to limit the Biometric Entry-Exit system, it will continue to expand beyond its original, claimed purpose

The current lack of regulation of biometrics and the associated technologies, particularly facial recognition technology, means there are little to no barriers to the continued expansion beyond the original purpose of the facial recognition identification system used for the Biometric Entry-Exit program. The Biometric Entry-Exit program itself demonstrates how the lack of regulation of biometrics has allowed the Government to use biometrics as it sees fit. Without consent or notice and a general lack of transparency at the beginning, CBP was able to obtain access to the millions of passport photos held by the State Department. CBP regular takes these photos to create biometric templates to use as part of their facial recognition identification system. There is no way to opt out of having your photo used this way and no one agreed to this.

Furthermore, the Biometric Entry-Exit program has continued to expand beyond its claimed original purpose to address visa overstays. CBP has made clear that it intends to expand the use of TVS, the backbone of its facial recognition identification system, for things like checking in for a flight. In a document obtained by EPIC through the Freedom of Information act, CBP described an airport process where every step from dropping off baggage, moving through TSA checkpoints, and boarding planes is mediated by facial recognition scans.[74] Additionally, FOIA documents obtained by EPIC show that other subcomponents of DHS, including Immigration and Customs Enforcement, the United States Secret Service, and the United States Coast Guard, will be able to leverage CBPs facial recognition identification system for their own mission operations.[75] There is no regulation is place that would stop CBP from continuing to expand access to its facial recognition identification system and leverage it for additional purposes.

VII. CBP'S OTHER USES OF FACIAL RECOGNITION TECHNOLOGY

It is worth noting that the Traveler Verification Service used as part of the Biometric Entry-Exit program is not the only CBP-owned facial recognition system. According to a GAO report, CBP's Automated Targeting System (ATS) is another system that incorporates facial recognition technology.[76] ATS has over 15 million photos in its database, including passport photos and State identification photos.[77] The ATS facial recognition system is used on individuals who: (1) Want to enter or exit the United States; (2) apply to CBP programs to travel to United States; or (3)

[74] Dep't. of Homeland Security, Biometric Pathway: Transforming Air Travel (Dec. 1, 2016), available at *https://epic.org/wp-content/uploads/foia/dhs/cbp/biometric-entry-exit/Biometric-Pathway.pdf.*

[75] Dep't of Homeland Security, Capability Analysis Study Plan for Biometric Entry-Exit (Jan. 23, 2017), available at *https://epic.org/wp-content/uploads/foia/dhs/cbp/biometric-entry-exit/Capability-Analysis-Study-Plan.pdf.*

[76] Government Accountability Office, Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks, 50 (June 2021), *https://www.gao.gov/assets/gao-21-518.pdf.*

[77] Id. at 50.

are “subjects of interest who require additional research and analysis.”[78] It is not clear who falls under this third category.

Additionally, CBP has used facial recognition systems “owned by Federal, State, local, and non-Governmental entities.”[79] We know that at least one of the non-Governmental entities is Clearview AI. According to reporting, CBP had close to 280 Clearview accounts registered that ran nearly 7,500 searches.[80] Clearview AI is one of the most controversial and dangerous implementations of facial recognition technology. Clearview secretly scraped billions of images from social media and other websites to create a massive biometric database.[81]

VIII. RECOMMENDATIONS

The safest and best thing for CBP to do would be for the agency to voluntarily cease using facial recognition technology. This would eliminate the risk of CBP’s facial recognition infrastructure being used for more pervasive surveillance or as a ubiquitous identification system.

But Congress should also act. Though I recognize it has not been referred to this committee, EPIC recommends that Congress enact H.R. 3907, the Facial Recognition and Biometric Technology Moratorium Act of 2021.[82] This bill would generally prohibit the use of facial recognition technology by CBP and other Federal agencies except for instances where Congress has explicitly authorized the use of the technology and provided robust protections. The Act would ensure there are protections against racial and gender bias and for privacy and First Amendment-protected rights. The Act would implement strong auditing and accountability requirements. In short, the Act would guarantee the type of protections that are currently lacking in CBP’s use of facial recognition technology and force Congress to carefully consider if CBP should implement facial recognition technology, and if so, how.

At minimum, Congress should put in place the following requirements for CPB’s use of facial recognition technology:

- The use of a one-to-one facial recognition identification system that does not require a database or connection to the cloud;[83]
- A prohibition on the use of facial recognition services (e.g. Clearview) provided by third parties;
- Prohibit CBP or other components of DHS or other law enforcement entities from using CBP’s facial recognition system for generalized investigative leads;
- Require CBP to only use its facial recognition system for identity verification as part of the Biometric Entry-Exit program and prohibit any other uses; and
- Require annual audits of CBP facial recognition system from an independent third party.

If the Biometric Entry Exit program is to remain in operation, these safeguards are critical to protect civil liberties, civil rights, and the security of sensitive biometric data.

IX. CONCLUSION

Facial recognition technology is a growing threat to our privacy, our civil liberties, and to our democratic values. EPIC urges Congress to address this technology in a meaningful way.

Thank you for the opportunity to testify today.

Chairwoman BARRAGÁN. Thank you for your testimony. I now would recognize Dr. Nicol Turner Lee to summarize her statement for 5 minutes.

[78] Id. at 50.

[79] Id. at 48.

[80] Ryan Mac, Caroline Haskins, and Logan McDonald, *Clearview’s Facial Recognition App Has Been Used By The Justice Department, ICE, Macy’s, Walmart, And The NBA*, Buzzfeed News (Feb. 27, 2020), *https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.*

[81] Kashmir Hill, The Secretive Company that Might End Privacy as We Know It, N.Y. Times (Jan. 18, 2020), *https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.*

[82] H.R. 3907, 117th Cong. (2021) (the Facial Recognition and Biometric Technology Moratorium Act of 2021 prohibits Federal agencies from using biometric surveillance systems without explicit authorization from Congress.)

[83] CBP has successfully tested the use of one-to-one facial recognition systems. A one-to-one system does not require a massive biometric database and virtually eliminates data breach risks and chance of that the system will be used beyond the original purpose.

STATEMENT OF NICOL TURNER LEE, PH D, DIRECTOR, THE CENTER FOR TECHNOLOGY INNOVATION (CTI), THE BROOKINGS INSTITUTION

Ms. TURNER LEE. Thank you, Chairwoman Barragán, Ranking Member Higgins, and distinguished Members of the House subcommittee. Thank you for this invitation to testify on the misuse of facial recognition by U.S. Customs and Border Patrol where I intend to center my concerns around diversity, equity, and transparency over how this technology is applied in various contexts. The Brookings Institution, with a history of a hundred years, is committed to evidence-based, nonpartisan research in a variety of focus areas.

The adoption and use of facial recognition by CBP has not come without challenges, largely because wide-spread micro surveillance in general has disproportionately hurt marginalized communities. Technology, the facial recognition technology, creates a privacy and bias concerns.

On a more general case, in 2021, a Black Michigan man sued the Detroit police for wrongfully arresting him as a shoplifting suspect after he was misidentified by facial recognition software. He was detained for hours and found innocent after not being the Black gentlemen in the grainy image whose face was clearly obstructed by personal effects.

Robert Williams is not alone is this less than optimal and accurate application of facial recognition. *The New York Times* has identified three instances which technology has led to the wrongful arrest of other Black men, which has been a likely occurrence to the misidentification, the technical inaccuracies when it comes to Black and Brown faces. Extensive research has also continuously pointed out that there is not the type of technical scrutiny needed to actually engage in more diversity, equity, and inclusion in these technologies.

With that, despite the tradeoffs that the agency has with regards to the efficiencies and effectiveness of processing travelers, it is important that it is not presumptuous in the regards to whether or not there is equity, diversity, and inclusion in the technical application as well as the sociological implications of the technology's use.

With that, I will read my testimony with recommendations to put before this committee as we consider appropriate use.

First, the agency must ensure transparency among travelers and other consumers subjected to face detection and recognition. As of now, while U.S. citizens can ensure that non-facial recognition identification information is properly stored and curated by the Department of Homeland Security, foreign nationals: not so much. We need to ensure that there is the same treatment of personally identifiable information with legal access and ability to amend those identification records, particularly our biometric data. We also need to ensure that CBP actually posts consistent messaging, informing all travelers of their rights when they are subjected to this technology.

Second, it is important to constantly optimize the technology with diversity, equity, and inclusion. The case of the gentleman in Detroit and countless other cases suggest that when this technology is applied in cases where it actually makes important eligibility determinations it has to be right. Government has been partnering with private-sector companies, such as Clearview and Vigilant, that implement facial recognition technology, but may not have these products reflect the lived experiences of the citizens that engage the product, meaning we need more diversity in Government as well as in the private sector to ensure that the empathy and technical agility to move across contexts that require a design, development, and deployment are representatives of other populations.

We also need to be aware that discrimination strategies—or anti-discrimination strategies for bias-mitigation be present when they are sold and procured by agencies like Customs and Border Patrol.

Third, we need to ensure and encourage wide-spread training for CBP professionals. The implementation and operation of facial recognition technology is done by human agents. However, a post-GAO report found that those agents did not have adequate training on what to do when the facial recognition does not work on a certain traveler or proper instruction on what to happen when a match is not found. Agents stationed at airports to assist travelers with the use of facial recognition should be adequately and constantly trained in understanding its limitations and biases and have an alternate strategy for processing.

Four, and my final recommendation, is that CBP should impose additional guardrails in instances where civil and human rights risk being violated. On my recent return from Berlin, Germany, I used facial recognition to bypass a long security line check. And though I was able to make my connecting flight, the trade-off is that I had no idea where my data was being collected, stored, and the potential for me to be denied entry as a result of the implicit and explicit biases that may have been apparent in the actual agent.

Members of Congress, for the agency to avoid front-page headlines it must encourage a constant interrogation of facial recognition, independent auditing, and think about those use cases where civil rights and human rights can be violated. Convenience should not be a trade-off for those important and critical aspects of our citizenry as travelers.

Thank you and I look forward to your questions for the remainder of this hearing.

[The prepared statement of Ms. Turner Lee follows:]

Prepared Statement of Nicol Turner Lee

July 27, 2022

Chairwoman Barragán, Ranking Member Higgins, and distinguished Members on the House Subcommittee on Border Security, Facilitation, & Operations, thank you for the invitation to testify as part of today's hearing on the use of facial recognition technology by the U.S. Customs and Border Protection (CBP), where I intend to center my concerns around diversity, equity, and transparency over how this technology is applied in various contexts. I am Dr. Nicol Turner Lee, senior fellow of governance studies, and director of the Center for Technology Innovation at the Brookings Institution. With a history of over 100 years, Brookings is committed to evidenced-based, nonpartisan research in a range of focus areas. My research encompasses data collection and analysis around regulatory and legislative policies that govern telecommunications and high-tech industries, along with the impacts of broadband access, the digital divide, artificial intelligence, and machine-learning algorithms on vulnerable consumers. My forthcoming book, *Digitally invisible: How the internet is* *creating the new underclass* (Brookings, 2022), addresses these topics and more. Today, I come before you with my own opinions.

CBP AND EMERGING TECHNOLOGICAL ADOPTION AND USE

As an agency, CBP is primarily responsible for border management and control. Responsibilities also lie around matters of custom and immigration, and the required verification of identities of travelers coming in and out of the United States. In 2013, CBP received funding to improve biometric identification and with that, moved to adopt facial recognition technology (FRT) to streamline existing matching processes, with the aim of modernizing and increasing efficiency for travelers and the Federal Government "without sacrificing safety and security by reducing the reliance on manual identity verification processes."[1]

Since its inception, CBP has been transparent in their adoption and use of facial recognition technologies as part of their National security efforts. Generally, the agency uses face detection and facial recognition technologies to confirm the identities of domestic and foreign travelers at Ports of Entry (POEs) for land, air, and sea borders. Over 187 million travelers have undergone such biometric screenings since its inception.[2] For air POEs, usually airports, CBP uses two processes, Simplified Arrival, for travelers entering the United States, and air exit, the program for travelers departing from the country.[3] As of December 2019, the CBP has spent $1.241 billion in the rollout of facial recognition technology, which is also referred to as "Biometric Facial Comparison Technology."[4]

However, the wide-spread adoption and use of FRT by CBP has not come without challenges. For my testimony, I focus on the intended and unintended consequences of FRT, and its implications for human rights and civil liberties that the agency should further consider as it expands these programs. In the spirit of common language before Congress and my fellow witnesses today, I define facial recognition technologies in accordance with the National Institute for Science and Technology, whose focus is on the comparison of "an individual's facial features to available images for verification or identification purposes.[5] I will offer three points in my statement regarding: (1) The general efficacy and accuracy of facial recognition technologies among diverse populations; (2) the sociological implications and trade-offs imposed on consumers when applied in commercial and public safety contexts; and (3) recommendations on what Congress and other policy makers can do to make these systems more fair, equitable, and responsible in the public safety/National security contexts. Taken together, these aspects of my testimony can help facilitate improved dialogs on how to make FRT more diverse, equitable, and fair, especially among subjects that are already over-surveilled due to their racial and ethnic differences, and other cultural stereotypes.

THE ACCURACY OF FACIAL RECOGNITION TECHNOLOGIES

Wide-spread and micro-surveillance has disproportionately hurt marginalized communities in the past, and facial recognition technology creates a range of privacy and bias concerns.[6] In 2021, a Black Michigan man sued the Detroit police for wrongfully arresting him as a shoplifting suspect, after he was misidentified by the facial recognition software used.[7] After being detained for hours, he was found innocent after not being the Black gentleman in the grainy image, whose face was clear-

[1] U.S. Department of Homeland Security. "Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies Report to Congress." August 30, 2019. *https://www.tsa.gov/sites/default/files/biometricsreport.pdf.*

[2] U.S. Customs and Border Protection. "CBP, Carnival Cruise Line introduces facial biometrics at Port of Baltimore." July 18, 2022. *https://www.cbp.gov/newsroom/local-media-release/cbp-carnival-cruise-line-introduces-facial-biometrics-port-baltimore.*

[3] Department of Homeland Security Office of Inspector General. *CBP Complied with Facial Recognition Policies to Identify International Travelers at Airports,* OIG–22–48. (Washington, DC, 2022). *https://www.oig.dhs.gov/sites/default/files/assets/2022-07/OIG-22-48-July22.pdf.*

[4] U.S. Customs and Border Protection. "Biometrics." Accessed July 21, 2022. *https://biometrics.cbp.gov/.*

[5] NIST. "Facial Recognition Technology (FRT)". February 6, 2020. *https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0#:?:text=Face%20analysis%20technology%20-aims%20to,for%20verification%20or%20identification%20purposes.*

[6] Turner Lee, Nicol and Caitlin Chin. "Police Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color." Brookings, April 7, 2022. *https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.*

[7] Harwell, Drew. "Wrongfully arrested man sues Detroit police over false facial recognition match." *The Washington Post,* April 13, 2021. *https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/.*

ly obstructed by some personal effects. Robert Williams, a 43-year-old father of two, sued the Detroit Police after this wrongful arrest in 2021, 1 year after the city approved a contract to extend its use of facial recognition software despite the misidentification of Black people. Williams is not alone in the less-than-optimal and accurate application of FRT. *The New York Times* identified three instances in which facial recognition technology have led to the wrongful arrests of other Black men—although the real number is likely much higher because some States do not require law enforcement to disclose when facial recognition technology is used to identify a suspect.[8] Such accounts of the misidentification of Black people by FRT have become more normalized. In its early stages of development, Rekognition, Amazon's facial recognition tool, falsely matched 28 Members of Congress to mug shots. While people of color made up only 20 percent of Congress at the same, they made up 40 percent of representatives that Rekognition falsely matched.[9] In response to these recurring failures, the ACLU quickly echoed concerns over its use, arguing that facial recognition technology has misidentified people of color in a range of application contexts, while placing civil liberties at risk by undermining citizen privacy.[10]

Extensive technical research and documentation have continuously pointed out the inefficiencies and inaccuracies of FRT when used to detect the biometric attributes of some diverse populations. For example, when used on women and historically marginalized communities, the results can be alarming. In February 2018, MIT, and then-Microsoft researchers Joy Buolamwini and Timnit Gebru published analyses of three commercial algorithms developed by Microsoft, Face++, and IBM. Their study found that images of women with darker skin had misclassification rates of 20.8 percent to 34.7 percent, compared to error rates of 0.0 percent–0.8 percent for men with lighter skin.[11] The researchers also noted biases perpetuated by training datasets, which disproportionately contained more lighter skinned individuals. 53.6 percent of the Adience dataset, 79.6 percent of the IJB–A dataset and 86.2 percent of the PBB datasets respectively consisted of lighter-skinned individuals.[12]

The National Institute of Standards and Technology (NIST), the agency responsible for testing FRT before market use, have also shown in recent assessments that with perfect lighting conditions, a fully cooperative subject, and no variation in the kind of camera used, some of the most advanced one-to-many FRT algorithms can exceed 99.5 percent accuracy when used for positive face matches. That is, when presented with multiple images of simulated passengers, at least 18 differently-studied algorithms could identify 99.5 percent of passengers accurately with a single presentation to the camera; results when the database only contained a single image of simulated passengers were less robust but still impressive, with 6 algorithms managing to meet or exceed the 99.5 percent accuracy threshold.[13]

While less favorable conditions for FRT use yield less reliable results, the general concern should be that FRT is not fully optimized for diversity, and equity in terms of highly representative and fair samples of subjects, particularly those from diverse backgrounds. Further, FRT can be both underwhelming and inconsistent, causing havoc to both subjects and the users of the said technology, like Robert Williams and the police officers that expressed a high level of certainty in his arrest.

[8] Hill, Kashmir (2020). Another arrest, and jail time, due to a bad facial recognition match. *The New York Times,* December 29. *https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html;* Valentino-DeVries, J. (2020, January 12). How the Police Use Facial Recognition, and Where It Falls Short. *The New York Times. https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.*

[9] Mak, Aaron. "Amazon's Facial Recognition Tool Screwed Up, Matched 28 Members of Congress to Mug Shots." *Slate Magazine,* July 26, 2018. *https://slate.com/technology/2018/07/amazon-face-matching-technology-misidentified-28-members-of-congress-as-criminals.html.*

[10] Ruane, Kate. "Biden Must Halt Face Recognition Technology to Advance Racial Equity/News & Commentary." American Civil Liberties Union, February 17, 2021. *https://www.aclu.org/news/privacy-technology/biden-must-halt-face-recognition-technology-to-advance-racial-equity.*

[11] Hill, Kashmir. "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match." *The New York Times,* December 29, 2020. *https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.*

[12] Buolamwini, Joy and 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. *https://proceedings.mlr.press/v81/buolamwini18a.html.*

[13] "NIST Evaluates Face Recognition Software's Accuracy for Flight Boarding." NIST, July 13, 2021. *https://www.nist.gov/news-events/news/2021/07/nist-evaluates-face-recognition-softwares-accuracy-flight-boarding.*

It has been argued that CBP's use of facial recognition software has undergone greater technical scrutiny to reduce the possibility of identification and matching for travelers. Yet, it is presumptuous to assume that the technology does not harness some of the same adverse effects, including those that disproportionately deny or detain travelers whose photos may be more difficult to discern, or whose demographic backgrounds may elicit both implicit or explicit biases when it comes to National security and border control.

While more than not, CBP FRT has been highly and strictly scrutinized on the technical levels, it does not suggest that the sociological implications of such data mining systems have been fully interrogated, leaving certain individuals more subject to greater surveillance and screening. The next section outlines use cases in policing, benefits eligibility, and education where FRT use has resulted in a series of intended and unintended consequences for consumers, which should advise CBP on its agency's own attempts for more diversity, equity, and accountability among its FRT systems.

Policing and law enforcement

In 2016, the Georgetown Law Center on Privacy and Technology found that law enforcement agencies across the United States have access to facial image databases encompassing over 117 million Americans, or over one-half of all American adults. They also concluded that one-quarter of all local and State police departments had the ability to run facial recognition searches despite facial recognition software demonstrating clear algorithmic bias.[14] As mentioned before, errors within facial recognition technology have led to multiple wrongful arrests of Blacks and even Hispanic populations as law enforcement becomes more dependent on these technologies in criminal instances and cases. In New York City, the number of arrests rose as more police officers used FRT—more than 2,800 arrests were made between 2011 and 2017, according to a 2019 Georgetown report.[15] From a societal perspective, higher arrest rates are normalized in Black and Hispanic communities due to more structural stigmas associated with these populations, resulting in the over-representation of their faces in law enforcement databases.[16] The National Association for the Advancement of Colored People (NAACP) reports that Black individuals are five times more likely than white individuals to be stopped by police officers in the United States, and that Black and Latino individuals comprise 56 percent of the U.S. incarcerated population but only 32 percent of the overall U.S. population.[17] This means that not only are police officers more likely to employ surveillance or facial recognition programs to compare images of Black and Latino individuals, but that mugshot images or arrest records of Black and Latino individuals are more likely to be stored in these databases in the first place. These two problems exacerbate existing patterns of racial inequity in policing.[18]

Public Benefit Identity Verification

Increasingly, States have also incorporated the use of facial recognition into identifying individuals' identities for the purposes of unemployment verification and accessing other social benefits. During the onset of the COVID–19 pandemic, many States moved to automate fraud detection as they were flooded with unemployment claims. In March 2020, 27 States entered contracts with ID.me, a private sector firm, to provide identity authentication through its facial verification software.[19] The use of this software proved controversial after the Internal Revenue Service dis-

[14] Garvie, C., Bedoya, A., & Frankle, J. (2016). Perpetual line up. Georgetown Law Center on Privacy and Technology, October 18. *https://www.perpetuallineup.org/background.*

[15] Johnson, Khari, March 7, 2022. The Hidden Role of Facial Recognition Tech in Many Arrests. *Wired Magazine, https://www.wired.com/story/hidden-role-facial-recognition-tech-arrests.* See also, Garve, Clare, May 16, 2019. Garbage In and Garbage Out. Georgetown Law, Center on Privacy and Technology, *https://www.flawedfacedata.com/#footnoterf49__ztly3aq*.

[16] Jennifer Lynch, "Face Off: Law Enforcement Use of Face Recognition Technology," Electronic Frontier Foundation, February 12, 2018, *https://www.eff.org/wp/law-enforcement-use-face-recognition.*

[17] "Criminal Justice Fact Sheet," NAACP, May 24, 2021, *https://naacp.org/resources/criminal-justice-fact-sheet.*

[18] Laura Moy, "A Taxonomy of Police Technology's Racial Inequity Problems," U. Ill. L. Rev. 139 (2021), *http://dx.doi.org/10.2139/ssrn.3340898.*

[19] Metz, R. (2021). Want your unemployment benefits? You may have to submit to facial recognition first. CNN, July 23. *https://www.msn.com/en-us/news/us/half-of-us-states-are-now-using-facial-recognition-software-from-this-little-known-company-to-vet-unemployment-claims/ar-AAMtC1Y?ocid=msedgntp.*

continued its use for tax returns and processing.[20] The State of Florida used FRT for unemployment verification—only to discover that older women and people of color were disproportionately more likely to encounter issues when using ID.me.[21] When facial verification failed, people would have to have a video call with a staff from ID.me. That involved waiting on the phone for more than 6 hours in the past, though the wait time had been reduced to 2 hours more recently.[22] Despite these flaws and other privacy issues, Florida and other States continue to use ID.me for benefits verification.[23]

Education

With the pandemic came the rise of on-line teaching and test proctoring. Such education software used FRT to help teachers monitor students and their behavior. However, racial biases in the software impacted this realm, making it more difficult for students of color to access these services. An investigation by Verge investigated Proctorio, failed to recognize Black faces more than half the time and failed to recognize faces of any ethnicity 25 percent of the time. Students of color using the software were unable to make the software detect their faces, and sometimes had to resort to measures such as shining flashlights on their faces to make themselves detectable.[24]

WE NEED A MORE DIVERSE AND EQUITABLE FRT ECOSYSTEM

Proponents of facial recognition use, and commercial actors argue the accuracy of facial recognition had grown over the years and had improved in their detection of women and Black and Brown people. Certainly, the best programs have identification rates in the high 90's. ID.me, which I previously mentioned in the determination of public benefit eligibility, touts a 95 percent success rate. However, that still means that 5 percent is failing. And of that 5 percent, a disproportionate number of them are women and people of color who have unequal access to these services. More must be done to improve the use of facial recognition technology to be optimal for all groups and applied contexts.

These and other examples of the ineffectiveness of facial recognition on darker skin tones point to the technical inefficiencies, which should also assert its lack of confidence when it comes to correctly identifying people traveling in and outside of U.S. borders. Such examples suggest that facial recognition technologies when applied in less-simulated, real-world contexts rarely have such a perfect confluence of conditions, leading to demonstrably lower accuracy rates.[25] In fact, standardization of photo conditions is an on-going topic of research, but real-world concerns remain.[26]

Further, it is widely established in a wide body of independent scholarship from researchers, including a recent study from NIST itself, that facial recognition technologies also have differential false negative and false positive rates across a variety

[20] Picchi, A., & Ivanova, I. (2022). ID.me says users can delete selfies following IRS backlash. CBS, February 9. *https://www.cbsnews.com/news/irs-id-me-delete-facial-recognition-tax-returns-backlash/.*

[21] Kylie McGivern, "Facial Recognition Blocks Legitimate Applicants from Unemployment Benefits," ABC Action News, June 11, 2021, *https://www.abcactionnews.com/news/local-news/i-team-investigates/facial-recognition-meant-to-stop-unemployment-fraud-is-blocking-legitimate-applicants.*

[22] Kylie McGivern, "Facial Recognition Blocks Legitimate Applicants from Unemployment Benefits," ABC Action News, June 11, 2021, *https://www.abcactionnews.com/news/local-news/i-team-investigates/facial-recognition-meant-to-stop-unemployment-fraud-is-blocking-legitimate-applicants.*

[23] Hurtibise, Ron, May 9, 2022. Florida continues to require identity verification with ID.me, Governing, *https://www.governing.com/security/florida-continues-to-require-identity-verification-with-id-me.*

[24] Mitchell Clark, "Students of Color Are Getting Flagged to Their Teachers Because Testing Software Can't See Them," The Verge, April 8, 2021, *https://www.theverge.com/2021/4/8/22374386/proctorio-racial-bias-issues-opencv-facial-detection-schools-tests-remote-learning.*

[25] West, Darrell M. "10 Actions That Will Protect People from Facial Recognition Software." Brookings, October 31, 2019. *https://www.brookings.edu/research/10-actions-that-will-protect-people-from-facial-recognition-software/;* Government Accountability Office. *Facial Recognition, CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues,* GAO–20–568. (Washington, DC, 2020), *https://www.gao.gov/assets/gao-20-568.pdf.*

[26] Grother, Patrick. "Face Standardization, Improving Face Recognition Via Specification of Images, Measurements on Images, Cameras." IFPC 2020, October 28, 2020. *https://pages.nist.gov/ifpc/2020/presentations/2b__grother__quality.pdf.*

of different demographics, including across race and gender.[27] As the recent 2019 NIST report shows, this happens both in one-to-one and one-to-many FRT matching; researchers reported that "demographic differentials present in one-to-one verification algorithms are usually, but not always, present in one-to-many search algorithms."[28]

THE IMPACT OF HAVING THE WRONG RESULT(S)

Negative effects of FRT have strong effects on historically marginalized communities.[29] For example, the NIST research team found higher rates of false positives for Black women, particularly in one-to-many matching. This is "particularly important," the NIST report noted, because the consequences of such higher rates of false positives "could include false accusations."[30] The research also determined that false positives, particularly in one-to-one matching, were between 2 and 5 times highest in women than men (varying by age, race, and algorithm used), and were higher in the elderly and children. NIST additionally reiterated a 2011 finding that the location of a developer was often a proxy for the race demographics of the data used in training.

False negatives (not finding a match to a true photo) had similar demographic differentials concerns in both one-to-one and one-to-many matching. These were also highest among Asian and American Indian individuals, and lowest in Black faces. Additionally, picture quality also plays a strong role—lower-quality images had significantly higher false negative rates than high-quality photos in good lighting, both as a reference image and to match against. The researchers note that these false negatives can often be remedied by taking a second picture, but this of course requires a fully cooperative subject—something not always possible with individuals intentionally attempting to deceive officials, including at the border.[31]

Anecdotal evidence of facial recognition errors highlights further evidence in discrimination. In 2015, Google apologized for mislabeling a picture of African American as gorillas.[32] In 2021, Facebook's AI categorized a video about Black men as "primates".[33]

But despite these proven inaccuracies, FRT is not only increasingly used, but with heavy reliance by law enforcement, including CBP officials, which has created a strong pipeline in terms of procurement—my last point worth mentioning before going into the recommendations. Clearview AI, who credentialed the CBP as one of many law enforcement agencies they work with, though CBP has separately claimed that Clearview AI's technology is not used for the biometric entry-exit program.[34] Clearview AI is one of the most prominent commercial providers of FRT to law enforcement agencies. Since 2017, the company has scraped billions of publicly-available images from websites including YouTube and Facebook, while enabling cus-

[27] Buolamwini, Joy and 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. *https://proceedings.mlr.press/v81/buolamwini18a.html.* Hachim El Khiyari and Harry Wechsler, "Face Verification Subject to Varying (Age, Ethnicity, and Gender) Demographics Using Deep Learning," *Journal of Biometrics & Biostatistics 7,* no. 4 (2016): 1–5, *https://doi.org/10.4172/2155-6180.1000323.* Patrick J. Grother, George W. Quinn, and P.J. Phillips, "Report on the Evaluation of 2D Still-Image Face Recognition Algorithms," *NIST,* June 17, 2010, *https://www.nist.gov/publications/report-evaluation-2d-still-image-face-recognition-algorithms.*

[28] Patrick J. Grother, Mei L. Ngan, and Kayee K. Hanaoka, "Face Recognition Vendor Test Part 3: Demographic Effects," *NIST,* December 19, 2019, *https://www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects.*

[29] Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," *The New York Times,* December 29, 2020, sec. Technology, *https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.*

[30] "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," *NIST,* December 19, 2019, *https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.*

[31] "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," *NIST,* December 19, 2019, *https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.*

[32] Conor Dougherty, "Google Photos Mistakenly Labels Black People 'Gorillas,'" Bits Blog, 1435791672, *https://archive.nytimes.com/bits.blogs.nytimes.com/2015/07/01/google-photos-mistakenly-labels-black-people-gorillas/.*

[33] Ryan Mac, "Facebook Apologizes After A.I. Puts 'Primates' Label on Video of Black Men," *The New York Times,* September 3, 2021, sec. Technology, *https://www.nytimes.com/2021/09/03/technology/facebook-ai-race-primates.html.*

[34] Ryan Mac, Caroline Haskins, Logan McDonald, "Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA," BuzzFeed News, accessed July 22, 2022, *https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.*

tomers to upload photos of individuals and automatically matching them with other images and sources in the database.[35] As of 2021, the private start-up had partnered with over 3,100 Federal and local law enforcement agencies to identify people outside the scope of Government databases. To put this tracking in perspective, the FBI only has about 640 million photos in its databases, compared to Clearview AI's approximately 10 billion.[36] Numerous other private corporations do work like Clearview, including Vigilant Solutions and ODIN Intelligence, who have provided law enforcement access to extensive databases for facial recognition.[37]

HOW FRT INACCURACIES IMPACT CBP AND TRAVELERS

According to a GAO report, the CBP only vets scans from two flights per airport each week, which could undermine their ability to monitor trends in inaccuracy.[38] Recognizing that inaccuracies in facial recognition often disproportionately hurt people of color, this means that they would face longer wait times for manual checks, or be subject to more extensive identity verification measures and searches. An examination of CBP's traveler verification service highlights some of the potential risks of bias.

Traveler Verification Service

Under the guise of the Traveler Verification Service (TVS), FRT is used from flight manifest data from commercial and private aircraft to build a photo gallery based on DHS databases built from traveler passports, visas, and other information that the U.S. Department of Homeland Security (DHS) has access to. The TVS technology takes a "live" photo of a passenger at an airport gate or security and compares this photo to all the photos in the DHS gallery. In 2 seconds, the system gives the agent a result: Match or no match.[39] There are different ways to search through photos with facial recognition technology, and this method of comparing the one live photo to the database is called a 1:N or one-to-many matching process.[40] Once there is a match, the agent decides if the traveler may legally enter or exit the country. If there is no match, then the agent will compare the passenger's live photo to a digital photo of the traveler's identification documents, which is called a 1:1 matching process. If there is still no match, the passenger will be subject to secondary inspection and considered a security risk.

U.S. citizens and some foreign nationals may opt out of this program, but it is mandatory for all foreign nationals aged 14–79. However, as GAO report documented, the opt-out process is not always clearly identified at gates using TVS.[41] CBP has made it clear that their goal is to document and track all passengers, in-

[35] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times,* January 18, 2020, *https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/#top17.*

[36] Eli Watkins, "Watchdog Says FBI Has Access to More than 641 Million 'Face Photos'," CNN, June 4, 2019, *https://www.cnn.com/2019/06/04/politics/gao-fbi-face-photos/index.html;* Will Knight, "Clearview AI Has New Tools to Identify You in Photos," *Wired,* October 4, 2021, *https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos/.*

[37] Max Rivlin-Nadler, "How ICE Uses Social Media to Surveil and Arrest Immigrants," The Intercept, December 22, 2019, *https://theintercept.com/2019/12/22/ice-social-media-surveillance/;* Conor Friedersdorf, "An Unprecedented Threat to Privacy," The Atlantic, January 27, 2016, *https://www.theatlantic.com/politics/archive/2016/01/vigilant-solutions-surveillance/427047/;* "Facial Recognition Technology: Current and Planned Uses by Federal Agencies," U.S. Government Accountability Office, August 24, 2021, *https://www.gao.gov/products/gao–21–526;* "Vigilant FaceSearch—Facial Recognition System," Motorola Solutions, accessed February 24, 2022, *https://www.motorolasolutions.com/en__us/products/command-center-software/analysis-and-investigation/vigilant-facesearch-facial-recognition-system.html;* Joseph Cox, "Tech Firm Offers Cops Facial Recognition to ID Homeless People," *Vice,* February 8, 2022, *https://www.vice.com/en/article/wxdp7x/tech-firm-facial-recognition-homeless-people-odin.*

[38] Government Accountability Office. *Facial Recognition, CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues,* GAO–20–568. (Washington, DC, 2020). *https://www.gao.gov/assets/gao-20-568.pdf.*

[39] Congressional Research Service. *Federal Law Enforcement Use of Facial Recognition Technology,* R46586, (Washington, DC, 2020). *https://crsreports.Congress.gov/product/pdf/R/R46586.*

[40] Department of Homeland Security Office of Inspector General. *CBP Complied with Facial Recognition Policies to Identify International Travelers at Airports,* OIG–22–48. (Washington, DC, 2022), 4. *https://www.oig.dhs.gov/sites/default/files/assets/2022-07/OIG-22-48-July22.pdf.*

[41] Government Accountability Office. *Facial Recognition, CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues,* GAO–20–568 (Washington, DC, 2020). *https://www.gao.gov/assets/gao-20-568.pdf.*

cluding U.S. citizens, from check-in, to baggage, to security,[42] to boarding the flight with ambitious performance goals to measure 97 percent of all exiting travelers on flights.[43] As the program's Privacy Impact Assessment states, "the only way for an individual to ensure he or she is not subject to collection of biometric information . . . is to refrain from traveling."[44]

TVS stores the biometric data on passengers that it collects in a computer system with the Office of Biometric Identity Management (OBIM), which collects biometrics through its Arrival Departure Information System (ADIS) on foreign nationals traveling in the United States in order to identify overstayers with TVS, as well as its Advance Passenger Information System (APIS), which contains arrival and departure manifest information to identify high-risk passengers, and Homeland Advanced Recognition System (HART), which is DHS's main biometric database that stores biometrics on non-U.S. citizens.[45] These systems aggregate data from multiple immigration databases, including from CBP, ICE, and USCIS.[46] The wide reach of data and sharing creates a significant interoperability challenge: ADIS combines data from five different CBP databases, an ICE system, a USCIS records system, a NPPD system, and information from data-sharing agreements with Canada and Mexico.

Once TVS compares the biometric data, it encrypts the photos into templates, which cannot be transformed back into photos. Currently, commercial partners cannot store the photos after they are transmitted to the TVS and can only see if the photo matches or not. However, initially, there were no limits on how commercial partners could use data, and it is unclear how DHS is monitoring their compliance without ever auditing most of their partners.[47] The data (including the live photos from TVS) is eventually stored in the DHS's Biometric Identity Management System (IDENT) and is kept for up to 12 hours for U.S. citizens, while foreign nationals' information is stored for up to 75 years.

There are many other databases that CBP maintains and collaborates on that are not incorporated directly into the TVS process currently. DHS and CBP cooperate with other Federal agencies and also have some access to local and commercial data systems to check for photo comparisons, including Michigan Law Enforcement Information Network (MLEIN), New York State Intelligence Center Photo Imaging Mugshot System (PIMS), Ohio Law Enforcement Gateway (OHLEG), Pinellas County Face Analysis Comparison and Examination System (FACES), and commercial FRT systems: Clearview AI, through an agent stationed at the New York State Intelligence Center, and limited access to Vigilant Solutions.[48]

While CBP has the capacity to audit its commercial partners, the lack of transparency of these audits and clear consent warnings for passengers does point to a larger problem of the TVS system, which is the lack of user control over the process and privacy transparency. There are also already political concerns in the United States. Bipartisan Senators Edward J. Markey (D–Mass) and Mike Lee (R–Utah) recommended that, "DHS should pause their efforts until American travelers fully understand exactly who has access to their facial recognition data, how long their data will be held, how their information will be safeguarded, and how they can opt out of the program altogether." A large group of Members of Congress expressed their concerns at the security risks posed for Americans in this program,[49] as there

[42] Transportation Security Administration. TSA Biometrics Strategy for Aviation Security & the Passenger Experience (Washington, DC, 2018). *https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.*

[43] Birnbaum, Emily. "DHS wants to use facial recognition on 97 percent of departing air passengers by 2023." *The Hill,* April 18, 2019. *https://thehill.com/policy/technology/439481-dhs-wants-to-use-facial-recognition-on-97-percent-of-departing-air/.*

[44] U.S. Department of Homeland Security. *Privacy Impact Assessment Update for the Traveler Verification Service (TVS): Partner Process,* DHS/CBP/PIA–030(c) (Washington, DC, 2017). *https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-june2017.pdf.*

[45] EPIC—Electronic Privacy Information Center. "*EPIC* v. *CBP* (Biometric Entry/Exit Program)." Accessed July 22, 2022. *https://epic.org/documents/epic-v-cbp-biometric-entry-exit-program/.*

[46] National Immigration Forum. "Biometrics at the Border," March 22, 2022. *https://immigrationforum.org/article/biometrics-at-the-border/.*

[47] EPIC—Electronic Privacy Information Center. "*EPIC* v. *CBP* (Biometric Entry/Exit Program)." Accessed July 22, 2022. *https://epic.org/documents/epic-v-cbp-biometric-entry-exit-program/.*

[48] Government Accountability Office. *Facial Recognition Technology, Current and Planned Uses by Federal Agencies,* GAO–21–526 (Washington, DC, 2021). *https://www.gao.gov/assets/gao-21-526.pdf.*

[49] Wild, Susan, Cleaver et al. "CBP Facial Recognition Letter," June 13, 2019. *https://wild.house.gov/sites/wild.house.gov/files/CBP%20Facial%20Recognition%20Ltr.%20final.-%20.pdf.*

is no direct legal basis for the air exit program targeting U.S. citizens, as the law establishing it only called for the surveillance of foreign nationals,[50] until former President Trump's Executive Order to verify the identity of all travelers at airports, including Americans.[51]

But the trade-offs to its non-use may result in longer wait times for passengers and an increased demand for agents that conduct manual checks. Thus, while there are inherent and potential privacy and civil rights concerns with this CBP program, the trade-offs of convenience resonate among agency staff and travelers who mitigate and give up their privacy and rights as part of the process. It is for these and other reasons that CBP and other agencies leveraging FRT must be on alert because a technology used for convenience should not have unforeseen consequences on travelers and citizens, more broadly. My testimony is not calling for a required ban on FRT, at least not currently or perhaps in the future. Rather, Congress and other stakeholders must thoroughly interrogate these models to ensure that they are not creating a new wave of systemic biases and discrimination.

WHAT CONGRESS AND OTHER POLICY MAKERS CAN DO TO IMPROVE FRT USE BY CBP

The fact of the matter is that if the Federal Government gets bias identification and mitigation wrong, it will erode the trust in the efficacy of autonomous systems, especially among everyday citizens whose lives are becoming more dependent on them. The use of FRT in the Federal Government—and especially at our Nation's borders—are no different. To reduce the disproportionate effect on historically marginalized groups, strike and maintain a balance between privacy and accuracy, and ensure the Customs and Border Protection agents securing America's borders understand limitations of facial recognition technology, I have a few proposals to offer the committee. First, the CBP should ensure transparency among travelers and other subjects of the technologies, especially the collection and storage of biometric data to maximize transparency on how their data will be used, while providing them the option to opt out. Second, technologists should improve inclusivity with existing use of facial recognition technology, to ensure that this technology works equitably across the lines of gender, age, race, and more. Third, on-going training should be provided to airport and CBP agents assisting travelers in using these tools. Finally, specific civil and human rights guardrails should be applied in cases known for bias. These recommendations to the CBP are further explicated below.

1. Ensure transparency among travelers and other consumers of FRT

Travelers must be made aware of the image storage, sharing, and curation process. As it stands, in the 2 years between May 2019 and September 2021, U.S. Customs and Border Protection used facial biometric technology deployed across 238 U.S. international airports to process 51.1 million travelers entering the United States; in total, more than 171 million travelers have been processed using facial recognition technology at air, land, and sea ports of entry.[52] The expansion of this Simplified Arrival program—which uses facial recognition technology to automate manual document checks required for entry into the United States—to all international airports across the United States was completed in June 2022, fulfilling a Congressional mandate to biometrically record entry and exit into the United States for non-citizens. As mentioned previously, photos of most foreign nationals entering the United States is stored in the Department of Homeland Security Office of Biometric Identity Management's Automated Biometric Identity System (IDENT) for 75 years, a length of time consistent with other existing CBP records with these photographs in IDENT, including full name, date of birth, country of residence, full passport information, U.S. destination address.[53] In contrast, images of U.S. citizens are

[50] Haskett, Mary. "Opting-out of Face Recognition at Airports." Medium, November 5, 2019. *https://austinstartups.com/opting-out-of-face-recognition-at-airports-bc01c3fa2361.*

[51] U.S. Department of Homeland Security and U.S. Department of Justice. "Executive Order 13780: Protecting the Nation From Foreign Terrorist Entry Into the United States Initial Section 11 Report." January 2018. *https://www.dhs.gov/sites/default/files/publications/Executive%20Order%2013780%20Section%2011%20Report%20%20Final.pdf.*

[52] "CBP Complied with Facial Recognition Policies to Identify International Travelers at Airports" (Office of the Inspector General, Department of Homeland Security, July 5, 2022), *https://www.oig.dhs.gov/sites/default/files/assets/2022-07/OIG-22-48-July22.pdf.*

[53] "Privacy Act of 1974; Department of Homeland Security/U.S. Customs and Border Protection–007 Border Crossing Information (BCI) System of Records" (*Federal Register,* December 13, 2016), *https://www.federalregister.gov/documents/2016/12/13/2016-29898/privacy-act-of-1974-department-of-homeland-security-us-customs-and-border-protection-007-border.*

not retained, and are instead deleted within 12 hours.[54] As of July 2022, most non-U.S. citizens must provide biometrics (with statutorily limited exceptions), although U.S. citizens cannotify a CBP officer to request manual identity verification if they do not wish to have their photograph taken.[55]

Pursuant to the 2016 final rule for the implementation of exemptions to the Border Crossing Information System of Records (which IDENT falls into), DHS has exempted parts of IDENT from disclosure under the Privacy Act. While individuals can access or amend records "with respect to information maintained in the system that is collected from a person at the time of crossing" the border, the DHS provides a litany of other privacy act exemptions that could and are used to share access to information contained within IDENT to other government and law enforcement agencies for a wide variety of reasons.[56]

In recent Federal privacy talks among U.S. legislators, there is an acknowledgement that data collection and use cannot be unlimited among the private and public sectors. Safeguards must be put in place, including through guaranteeing access to personally identifiable data, to prevent any privacy abuses by the Government or private entities, as a matter of fundamental rights. To that end, Federal, State, and local governments have enshrined privacy values into law—in certain contexts—through layers of Constitutional principles, limited statutes, and court cases. U.S. citizens and foreign nationals alike should have the ability to have their data handled in a manner consistent with these universally fundamental rights, but as it stands today, the Privacy Act of 1974 applies only to U.S. citizens. This lack of protection means that personally identifying information from most foreign nationals in the United States collected by IDENT (and other Government database systems) could theoretically be released by the Executive branch at any time and with minimal limitation.[57] While Presidential administrations have gone back and forth as to whether personally identifiable information from non-citizens should be treated in a manner consistent with what is mandated in the Privacy Act as a matter of politics, it is long past time for Congress to extend certain privacy rights for citizens to non-citizens and put the matter to rest, including the rights to access and amend their records of entry into the United States under the Privacy Act.[58]

As of now, while U.S. citizens can ensure that their non-facial-recognition IDENT information is properly stored and curated by DHS, foreign nationals have no way of ensuring that the same treatment is happening with their own personally identifiable information. With the legal ability to access and amend personal IDENT records—including accessing facial recognition data—Customs and Border Protection could post consistent messaging to all travelers informing them of their rights to access and amend if desired. Doing so could balance data accuracy concerns with National security biometric data collection needs from foreign nationals.

2. Optimize the technology for diversity, equity, and inclusion

The countless cases shared throughout my testimony suggest that more work needs to be done in these areas, starting with homogenous and less diverse developers deploying relevant facial recognition technology. Government agencies partner with commercial companies such as Clearview AI or Vigilant Solutions to implement facial recognition technology.[59] However, it is reported that public-private collaboration of facial recognition technology implementation makes it more difficult to detect

[54] "CBP Completes Simplified Arrival Expansion at All U.S. Airports" (U.S. Customs and Border Protection, June 2, 2022), *https://www.cbp.gov/newsroom/national-media-release/cbp-completes-simplified-arrival-expansion-all-us-airports.*

[55] "CBP Publication Number 1533–0921" (U.S. Customs and Border Protection, September 2021), *https://biometrics.cbp.gov/sites/default/files/docs/Air-Entry-Signage-24x36-English.pdf.*

[56] "Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Customs and Border Protection—007 Border Crossing Information System of Records" (*Federal Register,* March 21, 2016), *https://www.federalregister.gov/documents/2016/03/21/2016-06233/privacy-act-of-1974-implementation-of-exemptions-department-of-homeland-security-us-customs-and.*

[57] Esha Bhandari and Neema Singh Guliani, "The Trump Administration Is Threatening to Publicly Release the Private Data of Immigrants and Foreign Visitors," American Civil Liberties Union, February 28, 2017, *https://www.aclu.org/blog/privacy-technology/trump-administration-threatening-publicly-release-private-data-immigrants.*

[58] Lynn Dupree, "DHS PRIVACY POLICY REGARDING COLLECTION, USE, RETENTION, AND DISSEMINATION OF PERSONALLY IDENTIFIABLE INFORMATION," DHS Directive (Department of Homeland Security, May 4, 2022), *https://www.dhs.gov/sites/default/files/2022-05/DHS%20Mixed%20Systems%20Policy%20PII%20Instruction_1.pdf.*

[59] "Facial Recognition Technology: Current and Planned Uses by Federal Agencies," U.S. Government Accountability Office, August 24, 2021, *https://www.gao.gov/products/gao-21-526;* "Vigilant FaceSearch—Facial Recognition System," Motorola Solutions, accessed February 24, 2022, *https://www.motorolasolutions.com/en_us/products/command-center-software/analysis-and-investigation/vigilant-facesearch-facial-recognition-system.html.*

biases in the process. The Biometrics and Forensics Ethics Group (BFEG), an advisory non-departmental public body for the UK's Home Office, published a report that outlines ethical issues arising from the public collaborating with the private sector for implementing live facial recognition technology.[60] They found that if a public authority does not scrutinize the private entity's training dataset and algorithm, it is likely that discrimination and bias of the technology is exacerbated. Thus, they emphasize the importance of an independent oversight entity that can monitor the system.

There are multiple resources developed by academic researchers that could help Government agencies detect biases in FRT algorithms and potential harms. The "algorithmic impact assessment" by New York University's AI Now Institute help Government agencies or commercial companies to evaluate the accuracy, potential community harms or benefits, and risk of bias or discrimination before deploying any automated technology. Once the technology is in use, regular auditing that consider intersecting identities is an effective way to hold relevant companies accountable.[61]

Once biases in FRT are detected, multiple de-biasing measures could be implemented by scientists who oversee the datasets and algorithms. For instance, Jan Lunter suggested several methods to improve the accuracy of FRT.[62] In terms of the dataset, he proposed that data labeling based on rich and varied datasets and external dataset auditing could help make algorithms unbiased. There are multiple datasets available for algorithmic training created for the purpose of reducing racial and gender biases. Training the algorithm itself to detect biases through machine learning could be another solution mitigating bias.

What is essential is that the technology should not be left as a 'black box' in the hands of private entities. David Leslie of the Alan Turing Institute suggested several principles for building and using facial recognition technologies provide helpful guidelines.[63] First, he emphasized that a continuous chain of human responsibility must be established and codified that is traceable and auditable as a measure to ensure transparency and accountability across the entire design, development, and deployment workflow. Second, discrimination-aware strategies for bias-mitigation, both technical challenges arising from the dataset and sociotechnical challenges that arise from the development and deployment practices, should be incorporated holistically into the development and operation of FRT.

3. Ensure and encourage wide-spread training for CBP professionals

The implementation and operation of facial recognition technology is done by human agents. However, a past GAO report found that CBP officers do not have adequate training on what to do when facial recognition does not work on a certain traveler, or proper instruction or what to happen when a match is found.[64] Agents stationed at airports to assist travelers with using facial recognition technology should be adequately trained in understanding limitations and biases of the technology, to improve their understanding of racial biases in technology.[65] This also improves the customer service provided, ensuring that agents will not pose unreasonable demands to women and travelers of color who have difficulty utilizing these services. Instead, they could find helpful, constructive ways to see if there are other ways to activate the technology, and if not, utilize manual methods to verify the

[60] "Ethical Issues Arising from Public-Private Collaboration in the Use of Live Facial Recognition Technology", Biometrics and Forensic Ethics Group (BFEG), January 2021, *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment__data/file/953359/LFR__briefing__note__18.1.21.final.pdf.*

[61] Najibi, Alex. "Racial Discrimination in Face Recognition Technology." Science in the News, October 26, 2020. *https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology;* Raji, Inioluwa Deborah, Timnit Gebru, Margaret Mitchell, Joy Buolamwini, Joonseok Lee, and Emily Denton. "Saving face: Investigating the ethical concerns of facial recognition auditing." In Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, pp. 145–151. 2020. *https://dl.acm.org/doi/pdf/10.1145/3375627.3375820;* Reisman, Dillon, Jason Schultz, Kate Crawford, and Meredith Whittaker. *Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability.* (AI Now Institute, 2018).

[62] Lunter, Jan. "Beating the bias in facial recognition technology." *Biometric Technology Today 2020,* no. 9 (2020): 5–7, *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7575263/.*

[63] Zhang Yaobin and Weihong Deng, "Class-balanced training for deep face recognition", In *Proceedings of the ieee/cvf conference on computer vision and pattern recognition workshops,* pp. 824–825. 2020.

[64] "Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues" (U.S. Government Accountability Office, September 2, 2022), *https://www.gao.gov/products/gao-20-568.*

[65] Jessie Daniels, Mutale Nkonde, and Darakhshan Mir, "ADVANCING RACIAL LITERACY IN TECH" (Data & Society, May 2019), *https://datasociety.net/wp-content/uploads/2019/05/Racial__Literacy__Tech__Final__0522.pdf.*

identity of travelers. This ensures that the travel experiences of women and people of color will be smooth, despite inefficiencies in existing technology.

4. Impose guardrails in instances where civil and human rights risk being violated

While the recommendations discussed in this testimony are necessary preliminary steps, such as improving data set quality and training of TSA and CBP agents for administering this technology, many scholars, including those from international governing bodies and privacy advocates, conclude that facial recognition technology, in its current state, will never be a completely unbiased technology, and will always present privacy and civil rights risks. Access Now, joined by over 200 civil society organizations, signed a letter calling for an outright global ban on biometric recognition technologies, including FRT that enable wide-spread and discriminatory targeted surveillance.[66] But the problem is that even when FRT exhibits bias, it is simultaneously creating those other trade-offs previously discussed. On my return from Berlin, Germany a couple of weeks ago, I was able to bypass a long line at security check and go through a quick facial recognition scan instead in the midst of a growing and frustrating long line of travelers. As a society with deep historical wounds and trauma when it comes to systemic inequalities, lines should be drawn to get ahead of adverse effects of the technology, especially among agencies like CBP who may be in a greater spotlight among its peers. That is why, we must honor existing civil and human rights statutes and laws, while improve the technology through regular, independent audits, traveler transparency and feedback. CBP and other law enforcement organizations should work to improve current methods to ensure that they are equitable and just. When reviewing the CBP's air exit biometric program, the director of the Office of Test and Evaluation at the Department of Homeland Security found that while the program as it was lacked quantifiable benefits, it had the potential in the future when improved.[67]

Chairwoman Barragán, Ranking Member Higgins, and distinguished Members on the House Subcommittee on Border Security, Facilitation, & Operations, my testimony amplifies why and how CBP is not an exception to the various grumblings of FRT adoption and use. More must be done to improve equity and access to this technology, so that people of all ages, race, and gender could reap its benefits—they are also part of our democracy. Thank you again for the opportunity to testify, and I look forward to your questions.

Thanks to Brookings researchers Samantha Lai, James Seddon, Brooke Tanner, and Soyun Ahn for their assistance in preparing this statement.

Chairwoman BARRAGÁN. Thank you for your testimony. I now would like to recognize Mr. Daniel Tanciar to summarize his statement for 5 minutes.

STATEMENT OF DANIEL P. TANCIAR, CHIEF INNOVATION OFFICER, PANGIAM

Mr. TANCIAR. Thank you. Thank you, Chairwoman Barragán, Ranking Member Higgins, and distinguished Members of the subcommittee. I appreciate the opportunity to appear today to discuss CBP's use of facial recognition technology.

My name is Daniel Tanciar and I am currently the chief innovation officer at Pangiam. Prior to that, I was a CBP officer for 16 years, 12 of which I was at Headquarters. In 2016, until my departure in March 2020, I was the deputy executive director for the office responsible for biometric entry and exit transformation. I am here today in my personal capacity to share with the subcommittee my views and experience how CBP's use of facial recognition technology strengthens security, improves the international arrivals ex-

[66] "Open Letter Calling for a Global Ban on Biometric Recognition Technologies That Enable Mass and Discriminatory Surveillance" (Access Now, June 7, 2021), *https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Statement-English.pdf.*

[67] "Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues" (U.S. Government Accountability Office, September 2, 2022), *https://www.gao.gov/products/gao-20-568.* Nimra Khan and Marina Efthymiou, "The Use of Biometric Technology at Airports: The Case of Customs and Border Protection (CBP)," *International Journal of Information Management Data Insights 1,* no. 2 (November 1, 2021): 100049, *https://doi.org/10.1016/j.jjimei.2021.100049.*

perience, and increases operational efficiency in a manner that is consistent with privacy, civil liberties, and data protection principles.

Civil liberty and privacy protections were built into the program at the forefront. The program included opt-out provisions. It uses data already provided for international travel, limited data retention periods for U.S. citizens, and the requirement of posting of notices and signage. Photos are only taken with the traveler's knowledge with cameras that are in full view in places where persons must show their ID or travel documents today. This is not surveillance.

Additionally, CBP put forth business requirements to govern how airports, airlines, vendors, and other partners may interact with CBP's TVS and it outlines their responsibilities to safeguard data, participate in audits, and post notice to travelers about biometric processing.

CBP's technology does not determine identity. CBP officers make the final determination of identity. This technology is just one tool in a variety of others that CBP officers use in their mission. If a traveler chooses to opt out of the process, then traditional means of processing occur. It is swiping the passport and/or scanning the boarding card.

CBP has also worked with outside biometric experts, like the DHS Science and Technology Directorate, the Maryland Test Facility and the National Institutes of Standards and Technology to help them test, validate, and ensure optimal system performance. CBP chose a high-performing algorithm for TVS as measured by NIST's Face Recognition Vendor Test and evaluations. High-performing algorithms like the one used by CBP are incredibly accurate.

In the on-going work of NIST and the MdTF and others are key drivers of the significant rapid improvement in commercial algorithms today. Further, compared to human beings, algorithms can be more accurate. There are studies that show and suggest that Border Control officers, police, and banking employees who check IDs can experience error rates when matching unknown individuals as high as 30 to 40 percent in the challenging conditions in which they perform the task.

CBP's use of this technology strengthens security by reducing the imposter threat, those who use genuine documents that don't belong to them. Since 2018 through fiscal year 2021, CBP has identified over 950 of those imposters and they have been able to biometrically confirm over 100,000 overstays to their period of admission here in the United States.

The facilitation benefits are also important as this program for biometric exit was implemented in partnership with airlines and airports, with the goal of deploying technology that didn't just add another layer, but actually fit into the current operations and improved the travel process. One airline's biometric exit pilot demonstrated that facial recognition could save up 9 minutes of boarding per flight and another airline was able to board an A380 double-decker aircraft in about 20 minutes.

The entry system called Simplified Arrival begins with just a simple photograph. Rather than digging out your passport, handing it to the officer, the officer swiping the passport, and recollecting the same four fingerprints from returning visitors of the United States, the benefits to the CBP officer are less administrative work and more time to focus on the interview. Travelers benefit from reduced wait times and a simpler touch-free arrivals process.

In conclusion, over 100 million travelers have been successfully processed by CBP's use of this technology. While there are always improvements that can be made, CBP has implemented a well-performing program that meets the Congressional biometric mandate while maintaining privacy, civil liberties, and the data security foundation that it started from the beginning. It is through the continued oversight of Congress, the Government Accountability Office, the Inspector General, and continued CBP engagement with advocates that will continue to drive improvement and transparency about how the program is working and performing.

I look forward to answering questions. Thank you.

[The prepared statement of Mr. Tanciar follows:]

Prepared Statement of Daniel P. Tanciar

July 27, 2022, 2 o'clock PM

Chairwoman Barragán, Ranking Member Higgins, and distinguished Members of the subcommittee, thank you for the opportunity to appear today to discuss U.S. Customs and Border Protection's (CBP) use of facial recognition technology.

My name is Daniel Tanciar and since March 2020 I have been serving as the chief innovation officer at Pangiam, a company that applies computer vision and face recognition technology to define the future of trusted movement of people and goods.

Prior to joining Pangiam, I was a U.S. CBP officer in the Office of Field Operations (OFO) for 16 years. I spent 12 of those years assigned to CBP, OFO headquarters in Washington, DC. During my tenure at CBP, I worked on programs such as NEXUS, Global Entry, the Model Ports Initiative, the Immigration Advisory Program, and the CBP Mobile Program. From 2016 until my departure from CBP in March 2020, I was the deputy executive director for planning, program analysis, and evaluation, the office, at that time, responsible for Biometric Entry/Exit Transformation. In that role, I was part of the leadership team that implemented the use of facial recognition for biometric exit and entry.

I am here today, in my personal capacity, to share with the subcommittee my views and experience on how CBP's use of facial recognition technology at ports of entry strengthens security, improves the international arrivals experience, and increases operational efficiency in a manner that is consistent with privacy, civil liberties, and data protection principles.

BACKGROUND

In 2013, the biometric exit mission was transferred from DHS headquarters to CBP through the Consolidated and Further Continuing Appropriations Act of 2013 (Public Law 113–6). In 2017, CBP developed a process to use facial recognition as the means to implement biometric exit which has been mandated by Congress in multiple statutes over several decades.

The face recognition process for both entry and exit utilize existing advance passenger information (mandatory since the early 2000's) and photographs from passports, visas, other Federal documents, or previous border entries (which travelers have already submitted to the Government for the purposes of international travel) to build flight-specific galleries of photo templates for those travelers on that flight. Upon boarding the aircraft or arriving in the United States, a live photograph is taken of the traveler, securely transmitted to CBP's TVS, where it is matched against the gallery of templates. If the live photo is matched to the photo template of a U.S. citizen or another exempt category of traveler for biometric exit or entry the photo is deleted by CBP within 12 hours. If a photo is matched to the template of an individual in scope for biometric entry or exit the photo is retained and recorded as a biometric entry or exit record.

CIVIL LIBERTIES AND PRIVACY

When the biometric exit-entry process was designed, civil liberties and privacy protections were built into the program at the forefront and not as an afterthought. The program included opt-out provisions, photos were only taken in places where travel documents are required to be shown (e.g. security checkpoint, boarding gate, CBP primary inspection), and photos are taken with the traveler's knowledge with a camera in plain sight. CBP engaged with privacy advocates on several occasions, published multiple privacy impact assessments, engaged with the DHS's Data Privacy and Integrity Advisory Committee (DPIAC) and the U.S. Privacy and Civil Liberties Oversight Board (PCLOB).

Additionally, CBP developed business requirements to govern how airports, airlines, vendors, and other partners may interact with CBP TVS and outlines their responsibilities to safeguard data, participate in audits, and post notice to travelers about biometric processing.

CBP's facial recognition technology does not determine identity. CBP officers make the final determination of identity. The technology is just one tool that CBP officers can use to make admissibility or enforcement decisions. The results of a face recognition match or no match in and of itself is not used as a sole means to make these decisions. Likewise, for biometric exit, If there is no match or when a traveler opts out, then airlines simply revert to scanning boarding passes and reviewing travel documents to permit boarding.

FACIAL RECOGNITION PERFORMANCE

Early on, CBP recognized the need to work with outside biometric experts and organizations to help them test, validate, and ensure optimal system performance. In 2014, the DHS Science and Technology Directorate (S&T) and CBP opened the Maryland Test Facility (MdTF) to test and evaluate operational processes using biometric and non-biometric technologies. Since 2018, the MdTF has held biometric rallies that test and report on various biometric acquisition and matching technologies. The MdTF team has worked closely with CBP to identify best practices to measure and report on TVS performance. The MdTF team has also conducted and published research such as measuring demographic performance and race and gender impacts of identity (Maryland Test Facility, 2022).

CBP chose a high-performing facial recognition algorithm for the TVS as measured by the National Institute of Standards and Technology Face Recognition Vendor Test (FRVT) 1:1 and 1:N evaluations. These on-going face recognition evaluations are vital to monitoring continued algorithm performance and for monitoring for demographic differentials in facial recognition algorithms. The work that NIST and the MdTF are doing to test, measure, and report on algorithm performance is one of the key drivers of commercial facial recognition algorithm performance improvements over the last few years.

SECURITY BENEFITS

CBP's use of facial recognition technology strengthens security by reducing the imposter threat at the border and provides a higher level of accuracy of matching travelers to their ID documents.

Imposters to genuine documents are a documented border security risk that CBP officers must be vigilant against every day.

> "The use of documents by imposters, or look-alikes, is one of the simplest methods of passport fraud. An imposter will simply attempt to pass inspection at passport control by presenting a genuine, unaltered document issued to someone similar in facial appearance, and pretend to be that person to deceive the control officer . . . imposters are problematic for passport control because this type of fraud is difficult to detect and requires a high level of skill and professionalism in the examining officer." (Stevens, 2021).

While CBP officers must match unfamiliar travelers to the passports each day, studies suggest that Border Control officers, police, and banking employees who are relied upon to match IDs to live persons have the same error rates as novice reviewers (White, Towler, and Kemp, 2021). The novice error rates in pairwise face-matching tasks can be as high as 30 percent or 40 percent in challenging tests where images are captured in unconstrained environments (White, Towler, and Kemp, 2021). These error rates occur even when they are comparing IDs to people standing directly in front of them (White, Towler, and Kemp, 2021). When comparing the human error rate (30 percent–40 percent) for face matching to the error rate for face-matching algorithms (<3 percent), face recognition technology is more accurate and not subject to fatigue and other factors which may further increase the human error rate.

Since 2018 through fiscal year 2021 CBP's use of facial recognition technology has identified 46 imposters to genuine documents at U.S. airports and 916 imposters arriving at land ports of entry, and CBP has been able to biometrically confirm over 100,000 overstays (U.S. Customs and Border Protection, 2022).

FACILITATION BENEFITS

CBP's use of facial recognition began with the biometric exit program in the air environment that was implemented in partnership with airlines and airports with the goal of deploying technology in a way that fit into their current operations and improved the travel process. One airline's biometric exit pilot demonstrated that facial recognition could save up to 9 minutes per flight and another airline was able to board an A380 aircraft in about 20 minutes (Genter, 2019).

As face recognition began expanding from exit to entry in a program called Simplified Arrival, the administrative processes of handling the passport, matching the passport photo to the person standing in front of the officer, scanning the machine-readable zone of the passport, and re-collecting fingerprints from returning visitors to the United States could be replaced by the officer simply taking a photo of the traveler. The benefits to the CBP officer are the elimination of administrative processes, reduced handling of documents, and more time to focus on the traveler interview. Travelers benefit from Simplified Arrival with reduced wait times and a simpler touch free arrivals experience.

CONCLUSION

From fiscal year 2018 through fiscal year 2021 CBP has processed over 100 million individuals using face recognition technology. The use of facial recognition has led to the identification of over 950 imposters, improved aircraft boarding times, and enabled touch-free entry processing during the pandemic. While there are always improvements that can be made, CBP has made progress toward strengthening the program's privacy, civil liberties, and data security foundation. It is through the continued oversight of Congress, Government Accountability Office (GAO), the Inspector General, and CBP engagement with advocates that will continue to drive transparency about how the program is working and performing.

REFERENCES

Genter, K. (2019, April 23). *Your Guide to Biometric Boarding in the U.S.* Retrieved from The Points Guy: *https://thepointsguy.com/guide/biometric-boarding-us/*.

Maryland Test Facility. (2022, July). *Publications.* Retrieved from MdTF: *https://mdtf.org/Research/Publications*.

Stevens, C. (2021). Person Identification at Airports During Passport Control. In: *Forensic Face Matching,* Edited by Markus Bindemann, 8.

U.S. Customs and Border Protection. (2022). *CBP Trade and Travel Report Fiscal Year 2021.* Washington DC: U.S. Customs and Border Protection. Retrieved July 23, 2022, from *https://www.cbp.gov/sites/default/files/assets/documents/2022-Apr/FINAL%20FY2021__%20Trade%20and%20Travel%20Report%20%28508%20-Compliant%29%20%28April%202022%29__0.pdf*.

White, D., Towler, A., & and Kemp, R.I. (2021). Understanding Professional Expertise in Unfamiliar Face Matching. In: *Forensic Face Matching,* Edited by: Markus Bindemann, 62–68.

Chairwoman BARRAGÁN. Thank you for your testimony. Thank you too all our witnesses for their testimony. I will remind the subcommittee that you will have each 5 minutes to question the panel. I will recognize myself for 5 minutes and then we will alternate.

I will start by saying I have been myself through airports and have gone and used the program where they take the photo of you and it does speed up the process. There is no doubt about that. But I think I would have hesitation if I was one of those people that was misidentified or was held or arrested, and can understand the concerns that are being raised, and which is why we want to make sure we address those issues.

Ms. Gambler, I am going to start my questions with you. In 2020, GAO recommended that CBP develop and implement a plan to audit CBP's program partners for privacy compliance. At our subcommittee briefing earlier this month CBP informed us that the agency is conducting privacy audits of its commercial partners' use of biometric equipment in 7 locations. This seems like a very small sample to me. What is your reaction to CBP conducting privacy audits in only 7 locations?

Ms. GAMBLER. Thank you for the question, Chairwoman. We think it is positive that CBP has taken steps to implement these audits, but they do have a ways to go. They—to fully implement our recommendation need to audit partners not just in the air environment, but also in the land and sea environment. They need to ensure that they are conducting those audits on their contractors and vendors as well. So, they are taking some positive steps, but they still need to take more action to really implement our recommendation.

Chairwoman BARRAGÁN. Do you think that 7 is an appropriate number or think it is too small?

Ms. GAMBLER. We haven't had a chance to really understand sort-of what is going into these audits and how long they may be taking, but it is important that CBP continue down this path and make sure that they are auditing all of their partners, vendors, and contractors.

Chairwoman BARRAGÁN. What issues, controls, or practices should CBP assess when auditing airports, airlines, and other partners in their use of biometric equipment?

Ms. GAMBLER. They should be looking at both their privacy requirements as well as their security requirements and their implementation of those requirements.

Chairwoman BARRAGÁN. Then last, what actions must CBP take for GAO to close this privacy audit recommendation?

Ms. GAMBLER. They need to continue to implement the audits that they have planned and under way in the air environment, but they need to go further and also audit the partners that they are utilizing in the land and sea environments as well as contractors and vendors who are using personally identifiable information.

Chairwoman BARRAGÁN. Thank you. Dr. Turner Lee, NIST reports indicate that race and gender bias is statistically undetectable in the most accurate algorithms. This does not account for environmental factors. Could you talk about how this plays out in everyday life and the implications for those who are not able to be verified through facial recognition technology?

Ms. TURNER LEE. Yes, Chairwoman. I just want to confirm that you can hear me because the volume went lower.

Chairwoman BARRAGÁN. I can hear you.

Ms. TURNER LEE. We have seen in academic research journals that if the appropriate lighting is not actually confirmed or used on darker-skinned faces or if there are effects, like your glasses or a Black woman like myself who may change their hair, that there are likelihoods that the technical inaccuracies will allow for greater misidentification of an individual. So I think it is important that we acknowledge those technical inaccuracies generally when it comes to facial recognition technology use.

While we are seeing, and I think it was suggested and I will adhere, that there are greater levels of, you know, greater positives as opposed to false matches in some cases. Let me continue to remind folks a study of a facial recognition software a couple years ago misidentified a majority of Members from the Congressional Black Caucus as mug shots simply because the technology has not yet been optimized for diversity in complexion, in effects, in lighting, et cetera. That is the criteria I think that we still need to apply and interrogate if we are going to use these systems in a steady manner.

Chairwoman BARRAGÁN. Thank you. Mr. Scott, how would you describe Customs and Border Protection's oversight efforts to maintain data privacy of travelers? What recommendations would you give to CBP in order to help protect—to help travelers feel that their data is protected?

Mr. SCOTT. Well, I think the data breach I mentioned earlier is evidence that the privacy and security protocols are lacking. You know, CBP does use one-on-one facial recognition which doesn't require a database. They have tested that. That is where, you know, you would take your Government-issued document like a passport and the image on there would be scanned, and then compared to a real-time photo of yourself. No database needed. No connection to the cloud. After that scanned in—after the confirmation identification—after your identity is confirmed, then that information is erased. The biometric data is not kept. It is a much safer way to implement the use of facial recognition.

Chairwoman BARRAGÁN. Thank you. Thank you, Mr. Scott. My time has expired. So now I will now recognize the Ranking Member of the subcommittee, the gentleman from Louisiana, Mr. Higgins, for questions.

Mr. HIGGINS. Thank you, Madam Chair. Mr. Tanciar, one of the witnesses mentioned, he spoke of a data breach where 184,000 images of travelers were stolen essentially from CBP. Are you familiar with that case?

Mr. TANCIAR. Yes, sir.

Mr. HIGGINS. OK. Let us dig into that a little bit now because obviously it was a criminal action and outside the parameters of any kind of contractual agreement. We, all Americans, are familiar with data theft and that sort of behavior is something that we have all learned to be quite cognizant of and we take some extreme measures to protect our data.

So, let us talk about the database itself. Maybe you can help clarify that for the committee. Explain to America how images are collected, whether or not the collection is voluntary. The database which is used for comparisons as travelers come through the system and are part of the facial recognition technology assessment of who they are, exactly where does the database come from?

Mr. TANCIAR. Certainly, Mr. Higgins. For the system as a whole and the area where the data breach occurred was a very one-off pilot of equipment in Anzalduas, Texas, where somebody actually had to insert a USB drive, who had access, submitted work tickets, all contrary to their training and contractual obligations. So that incident——

Mr. HIGGINS. It was a criminal act, right?

Mr. TANCIAR. In my view, it is a criminal act.

Mr. HIGGINS. Right. I am sure it was investigated. But the database itself for all facial recognition technology——

Mr. TANCIAR. Yes, sir.

Mr. HIGGINS [continuing]. Explain to America how we collect those images, those photographs, and whether or not that is voluntary.

Mr. TANCIAR. So, everybody who travels internationally, whether it be a U.S. citizen, a person visiting the United States, you have to either have a passport in which you submit a photograph to the U.S. State Department for or you apply for a visa, which you also submit that to the State Department. That information is available to U.S. CBP.

When flights are coming or leaving the United States, there is manifest data that is transmitted by the airline that permits CBP to match that manifest data to the travel document information on there.

Mr. HIGGINS. OK. So, using the same—I just wanted to clarify for the citizenry that we serve, we are talking about a technology for facial recognition that compares the image of the traveler with the already available and willingly provided a photographic image of that person that they are stating that this is me.

Mr. TANCIAR. That is correct.

Mr. HIGGINS. It is, OK. So, what happens if a traveler is falsely identified? They are in the line, they are falsely identified, or if there is a failure to identify, what exactly happens to that person?

Mr. TANCIAR. So, if you are departing the United States and a No Match is returned, the regular process ensues. So, the gate agent will verify your passport or travel document.

Mr. HIGGINS. They will ask them to step out of the line and show their passport?

Mr. TANCIAR. Yes. Normally, that doesn't happen where they step out of line. It happens pretty quickly. If there is a Failed/No Match at least my observation is that they look at the passport, they scan the boarding card, and on to the plane they go.

Mr. HIGGINS. That is it?

Mr. TANCIAR. That is it for biometric exit.

Mr. HIGGINS. Well, can you think of any reason why there would be objections to full deployment of this technology as it currently exists, recognizing the fact that it has come a long way in the last decade and certainly it is advancing as we speak? I mean, there is an image that has been presented to the citizens that we serve that this is some sort of a nefarious technology and there is Big Brother watching you. But really it is using photograph images that travelers willingly have provided. They are available on their passport, a visa, driver's license. We already have that information. It just speeds up the traveler's passage through a security checkpoint. If for some reason their image is not recognized or they are flagged with a false identity, they are pulled out of the line, and they go through the normal check with a human being. Is that correct?

Mr. TANCIAR. Yes, sir, that is correct.

Mr. HIGGINS. Madam Chair, I am encouraged that we are having this hearing. I think we are moving toward some common ground here, which is far too uncommon in this body. So, thank you for holding the hearing and I thank our witnesses.

Chairwoman BARRAGÁN. Oh, well, thank you, Ranking Member. The Chair will now recognize other Members for questions they may wish to ask the witnesses. As previously outlined, I will recognize Members in order of seniority, alternating between Majority and Minority. Members are reminded to unmute themselves when recognized for questions.

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

Ms. CLARKE. I thank you, Madam Chair, and I thank our Ranking Member and I thank the very distinguished panelists this afternoon for sharing your expertise with us.

Congress directed the consumer—excuse me, the—I am sorry, the Consumer Border Protection Agency to collect biometrics from non-U.S. citizens as part of the Entry-Exit Program. However, Congress did not specify which biometric the agency should use. I am sorry, directed the Customs and Border Protection Agency, I had a mistake there. Congress did not specify which biometric the agency should use. In terms of privacy and risk of surveillance facial recognition is one of the most problematic biometrics to implement.

Mr. Scott, if facial recognition algorithms are only highly accurate under ideal conditions, should CBP continue investing in facial recognition technology from biometric entry and exit?

Mr. SCOTT. Obviously, you know, how accurate the algorithms work need to be tested on an on-going basis. If they are not accurate, it is one reason not to use it, but it is not the only reason because ones will get better. Right? But they can—you know, our larger concern is the implementation of a facial recognition system in the first place, you know, the Government using photos that U.S. citizens gave to get a passport. That is why I gave my photo over to get a passport, to have control over my identification. With facial recognition the Government is taking control over identification. It becomes a universal ID that is part of the pier where the Government now controls the ability to identify you when they want, with your consent, without your consent, with your knowledge, or without your knowledge. That is kind-of a larger concern, particularly when there are no kind-of overarching regulations in place to prevent the expansion of this program.

Ms. CLARKE. Are there other biometric systems that can be adopted instead of facial recognition that ensure travelers' privacy is protected and are more accurate and secure? Mr. Scott.

Mr. SCOTT. Well, the CBP has tested other ones: Fingerprint, iris. You know, a fingerprint is a pretty accurate technology. It has been around for a long time.

My understanding from the documents I have read, through the Freedom of Information Act documents EPIC has received, the stuff posted by CBP, my meetings with CBP that they went with facial recognition in large part because it was easy. The fact that it was easy is actually one of the concerns here for the potential expansion of the program because it is easy to expand. It is easy to take a facial recognition system and then use it for other purposes beyond the initial purpose for the implementation of the program in the first place. It can be connected to other sources of data, other photos in a very easy manner. Without, you know, again, proper regulations in place, it is just bound to expand. That is why EPIC has recommended not using facial recognition. If facial recognition is going to be used, to use a one-on-one system instead of a one-to-many.

Ms. CLARKE. OK. Many U.S. citizens confronted with CBP's FRT biometric entry-exit system at Customs may not be aware that they have the right to opt out, especially if there isn't sufficient or visible signage at key points throughout the exit-entry process to alert them of this right. Additionally, some travelers may be concerned or even afraid of what will happen if they opt out.

So, my next question is for Ms. Gambler. Along with complying with GAO's recommendation for pre-signage, what else can Congress and CBP do to ensure traveling U.S. citizens are not only clearly aware of their right to opt out of FRT, but also fully understand what the process is after and there will not be a any repercussions if they are to opt out?

Ms. GAMBLER. Yes. Thank you for the question, Congresswoman. Your question really speaks to one of the key findings from our report, which is that CBP needs to make sure that the notices, whether that is signs or through other mechanisms that CBP uses to inform the public about the Biometric Entry-Exit Program and use of facial recognition technology, that all of those mechanisms for notifying the public provide clear, complete, accurate information about the ability of eligible travelers to opt out of the facial recognition technology. That should include information about alternative screening that individuals, that travelers could go through. Also, to be clear that there aren't any consequences from opting out of the use of facial recognition technology.

So, those things, making sure that that information is complete across all of CBP's different notice mechanisms and that it is available particularly where facial recognition technology is being used, those things are important.

Ms. CLARKE. Thank you. I yield back. I have overrun my time. Good to see you, Ms. Turner. To everyone else, have a pleasant day. I yield back, Madam Chair.

Chairwoman BARRAGÁN. Great. Thank you to the Representative from New York. I now recognize the gentlewoman from Texas, Ms. Flores. You are recognized for 5 minutes.

Ms. FLORES. Thank you, Madam Chair and Ranking Member Higgins, for holding this hearing today. Thank you to all the witnesses for being here today as well.

I firmly believe that the facial recognition technology has the potential to play a vital role in our country's National security going forward, specifically combating cartels, terrorists, drug smugglers, and child sex traffickers. That being said, as Congress we need to ensure that the appropriate guardrails are in place concerning the use of this technology and that the data collected with it, to make sure we are balancing legitimate public safety concerns with the individual's privacy and liberty.

The question is for Ms. Gambler. Could you please elaborate on how law enforcement officers and agencies are able to utilize biometrics and facial recognition technology to specifically counter cartels, terrorists, drug smugglers, and child sex traffickers?

Ms. GAMBLER. Yes. Thank you for the question, Congresswoman. That has not been specifically part of the work that GAO has done, looking at the CBP's use of facial recognition technology for the Biometric Entry-Exit Program.

But what I can say is as it relates to CBP's use of facial recognition technology within the Biometric Entry-Exit Program CBP has identified benefits to its use. It helps automate the traveler identification verification process. It can help expedite that process. It also helps CBP to detect potential use of fraudulent travel documents, for example. So, within that environment of the Biometric Entry-Exit Program, CBP does identify benefits from the use of facial recognition technology.

Ms. FLORES. Another question, could you specifically give me statistics on the number of times that the biometrics and facial recognition technology has successfully stopped instances of human trafficking?

Ms. GAMBLER. I don't know if that specific data is available, Congresswoman, but we would be happy to follow up on what data CBP may have on its efforts and provide you a response back after the hearing.

Ms. FLORES. I would love that. Thank you so much. Thank you, Madam. I yield my time.

Chairwoman BARRAGÁN. Well, thank you. I am going to go ahead and go for a second round for anybody who wants to ask any questions.

Mr. Tanciar, I am curious if you have any information or data, do you know how often the system, whether it is at the land port of entry or seaports or airports, how often a person is identified as like a possible person of a cartel? Like do we know if it is like 5 percent or 10 percent or less than 1 percent? Is there any data we—somewhere we can look for that data?

Mr. TANCIAR. Unfortunately, I don't have that data.

Chairwoman BARRAGÁN. Yes.

Mr. TANCIAR. I am not aware of where that data exists. The system has been used to match people to their identity documents. While there certainly have been identifications of nefarious and bad actors, there is a culmination of data that goes into that identification, not just face recognition.

Chairwoman BARRAGÁN. Right. I am just curious, like if I am, you know, a bad actor, am I going to go through the biometrics or, you know, find another way to avoid it? So I was just curious on how often it might come up, and that may be something I will just kind-of follow up and see where we may be able to get that data.

My next question, Dr. Turner Lee, since many of the facial recognition technologies are procured by Federal agencies, how do we make the private sector more accountable to developing more inclusive and representative technologies?

Ms. TURNER LEE. Chairwoman, that is a great question and thank you for the opportunity to answer. I think what is most important here despite the fact that we are seeing a high technical success rate with the software in question, that we have to ensure that the private sector, who ultimately is where we are procuring not only the faces, but some of the technologies that run the backhaul of these systems, that they have a couple of principles in mind.

In addition to privacy and security, they should also have diversity and equity on their team. They should be regularly committed doing types of third-party audits, civil rights audits, audits for disparate treatment or impact of their product. Working alongside the agency, there should be a common goal of ensuring that there is no technical breakdown and sociological implication of its use.

The only thing that I would really share in this comment to you, Chairwoman, is that we are again presumptuous to think that just because the technology is able to process travelers at its full capacity, we have not seen to this date any technology that has not had its share of complications. When we pull back from interrogating those technologies is when we actually receive the worst of its outcomes on innocent people.

So I do think the private sector, in partnership with CBP, has a responsibility to share and demonstrate the type of transparency, accountability, as well as security, diversity, and equity in their own business practices and models.

Chairwoman BARRAGÁN. Thank you. Mr. Scott, how can we raise awareness among travelers about the potential trade-offs of their rights and the conveniences associated with expediting identification and verification process for travelers?

Mr. SCOTT. Well, one, as mentioned before, the signage needs to be more visible. A lot of times people don't see the signs about the use of facial recognition or the potential to opt out if you are a U.S. citizen. But they also need to know actually before, before going to the port, before going to the airport or any other port of entry.

It is hard to really process and think about the consequences of submitting to facial recognition when you are actually at the airport traveling. It is a high-stress situation. You usually just want to kind-of get from point A to point B and get through security lines, et cetera, so people need to understand prior to that. So, there needs to be an information campaign to inform people prior to them traveling, so they understand more about the use of facial recognition.

But also, you know, with the lack of regulations right now, you know, it is arguably impossible for people to actually understand the complete possible consequences of submitting to facial recognition because it is impossible to think about. What type of mission creep will happen in terms of what will this information be used for down the road? How will facial recognition be implemented in the future? Will it become a universal identification controlled by the government, further creating that asymmetry of power between the individual and the Government?

Chairwoman BARRAGÁN. Thank you. Dr. Turner Lee, do you have anything you want to add to that?

Ms. TURNER LEE. Yes, I completely agree. I mean, not only do we have to have signage available before people go to the airport, we have to be culturally sensitive. This goes back, again, to having some level of lived experiences of the populations that are being surveilled by this technology.

Signage needs to be in Spanish, in multiple languages; be accessible to people with disabilities. I think we are, again, assuming that most people understand how the technology is being used in light of the trade-off of convenience. I think that is a very core assumption for us as Federal stewards to ensure that we are not in some way, either now or in the future, intruding upon people's civil and human rights.

Chairwoman BARRAGÁN. Well, thank you. I do think it is an interesting conversation because, in my mind, the Government already has my California driver's license photo, it has my passport photo. Yet, as a traveler, I am looking for convenience and speed and how quickly can I go. So I think that there has to be that conversation of the trade-offs.

I just do wonder, too, how much longer you would go through security if you decided to opt out versus, you know, just doing the biometrics?

So a lot more discuss, but, Representative Higgins, the floor is yours for your second round.

Mr. HIGGINS. Thank you, Madam Chair. Mr. Tanciar, I am going to ask you about exactly what happens when you encounter an imposter. Referencing what the other gentleman described as not having control, his ID, and, you know, you have your passport he stated, and I have control of my ID, but in the facial recognition technology the Government has control of your ID. Again, it paints quite a nefarious picture.

But may I say, I was a police officer for a long time before I came to Congress. It was an everyday affair that you had interaction with someone that did not have their driver's license with them to identify themselves. It was not an uncommon encounter that that person had something to hide, usually they had a warrant. They would lie about their identity. They would give you a name and date of birth, usually of a friend or a family member that they knew was clean and did not have warrant, and they could be quite convincing. Quite convincing.

But if you had some time on the street you could pick up the vibes that they were lying and you would call it in to dispatch. Send me a picture. They would send it to your phone of the—you would run a driver's license by name and ID, which you can do, and dispatch would send an image of that driver's license to my phone. So, now I had the picture of the guy he said he was. I would show it to him and say that is not you, man. Why don't you tell me who you really are and what your warrant is for? And we would move forward.

So, to think, to State, to insinuate that law enforcement doesn't have your image in the computer is just not reality. So, what happens when you encounter—say you encounter 1,500 imposters. The facial recognition technology is pretty good at picking up someone that is attempting to use someone else's identity. What happens exactly if you encounter an imposter?

Mr. TANCIAR. Well, it is a multi-layered effort. The first instances of the photo being taken and a no-match being returned, we will then go to a one-to-one against the document. Then if one-to-one against the document doesn't return anything——

Mr. HIGGINS. Again, it is a document that the traveler has in his possession?

Mr. TANCIAR. Has in their hand. That is correct, has in their hand, which could—might not be theirs.

Mr. HIGGINS. Right.

Mr. TANCIAR. It is a document that they have obtained because they felt they looked enough like a person on the document and they were trying to pass that off for entry. You know, CBP officers would work long, hard hours and have a very important task. Sometimes people are good at that, looking like what is on the document. But the facial recognition technology helps identify that up front, but that doesn't make the decision.

Then there is a whole process of interviewing. Where did you get the document? How did you obtain the document? What street did you grow up on? There is lots of factors.

Mr. HIGGINS. That is an interesting point because the streamlined checkpoint that facial recognition technology provides, does it allow the agents to spend more time in the interview process if they have someone that needs to be questioned?

Mr. TANCIAR. Yes, it does. Those administrative processes of handling the documents and looking at a one-by-one square to the person standing in front of you is automated. That gives me, the officer, more time to ask the questions that are important about the purpose and intent of the travel.

Mr. HIGGINS. OK. Madam Chair, I very much appreciate you holding this hearing today. I thank your witnesses for appearing.

I thank Ms. Gambler. I have another question I would like to submit to you, ma'am, it is a little more extensive, in writing after the hearing. My office will deliver that, if that is OK. I very much appreciate your attendance.

Ms. GAMBLER. We look forward to the question and happy to provide a response.

Mr. HIGGINS. Yes, ma'am. Thank you, Madam Chair. I yield.

Chairwoman BARRAGÁN. Thank you. I want to thank the witnesses for their valuable testimony and the Members for their questions. The Members of the subcommittee may have additional questions for the witnesses and we ask that you respond expeditiously in writing. Without objection, the committee record shall be kept open for 10 days.

Hearing no further business, this subcommittee stands adjourned.

[Whereupon, at 3:02 p.m., the subcommittee was adjourned.]

○