TESTIMONY OF NICOL TURNER LEE
Director, Center for Technology Innovation, The Brookings Institution
Senior Fellow, Governance Studies, The Brookings Institution

Before the United States House of Representatives
Committee on Homeland Security
Subcommittee on Border Security, Facilitation, & Operations

Hearing on "Assessing CBP's Use of Facial Recognition Technology"

Mitigating Bias and Equity in Use of Facial Recognition Technology by the U.S. Customs and Border Protection

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 U.S., 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 widespread 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

[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/.

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 policymakers 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 dialogues 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

Widespread 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 clearly obstructed by some personal effects. Robert Williams, a 43-year-old father of two, sued the Detroit Police after this

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

wrongful arrest in 2021, one 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% of Congress at the same, they made up 40% 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% to 34.7%,

[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.

compared to error rates of 0.0%-0.8% for men with lighter skin.[11] The researchers also noted biases perpetuated by training datasets, which disproportionately contained more lighter skinned individuals. 53.6% of the Adience dataset, 79.6% of the IJB-A dataset and 86.2% 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% 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% 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 six algorithms managing to meet or exceed the 99.5% 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.

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

---

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.

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 U.S. 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,

[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

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 U.S., and that Black and Latino individuals comprise 56% of the US incarcerated population but only 32% 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 data bases 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 discontinued its use for tax returns and processing.[20] The state of Florida used FRT for unemployment verification – only to discover

[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.
[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/.

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 six hours in the past, though the wait time had been reduced to two 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 online 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% 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 90s. ID.me, which I

[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.

previously mentioned in the determination of public benefit eligibility, touts a 95% success rate. However, that still means that 5% is failing. And of that 5%, 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 ongoing 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 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

[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.

[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.

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

[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.

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 customers to upload photos of individuals and automatically matching them with other images and sources in the database.[35] As of 2021, the private startup had partnered with over 3,100 federal and local law enforcement agencies to identify people outside the

[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 McDonald Caroline Haskins, Logan, "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.
[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.

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

[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.

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 two 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, including U.S. citizens, from check-in, to baggage, to security,[42] to boarding the flight with ambitious performance goals to measure 97% of all exiting travelers on flights. [43] As the program's

[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.
[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/.

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 U.S. 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)

[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/.

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 is no direct legal basis for the air exit program targeting U.S. citizens, as the law

[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 eta al. "CBP Facial Recognition Letter," June 13, 2019. https://wild.house.gov/sites/wild.house.gov/files/CBP%20Facial%20Recognition%20Ltr.%20final.%20.pdf

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 tradeoffs 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 tradeoffs 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 policymakers 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

[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.

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, ongoing 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 two 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 seaports 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

[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),

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 can notify 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

https://www.federalregister.gov/documents/2016/12/13/2016-29898/privacy-act-of-1974-department-of-homeland-securityus-customs-and-border-protection-007-border.

[54] "CBP Completes Simplified Arrival Expansion at All US Airports" (US 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-securityus-customs-and.

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

[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.

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 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]

---

[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.

[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).

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 widespread 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

[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.

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 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 widespread and discriminatory targeted surveillance.[66] But the problem is that even when FRT exhibits bias, it is simultaneously creating those other tradeoffs 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

[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.
[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.

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.

[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.