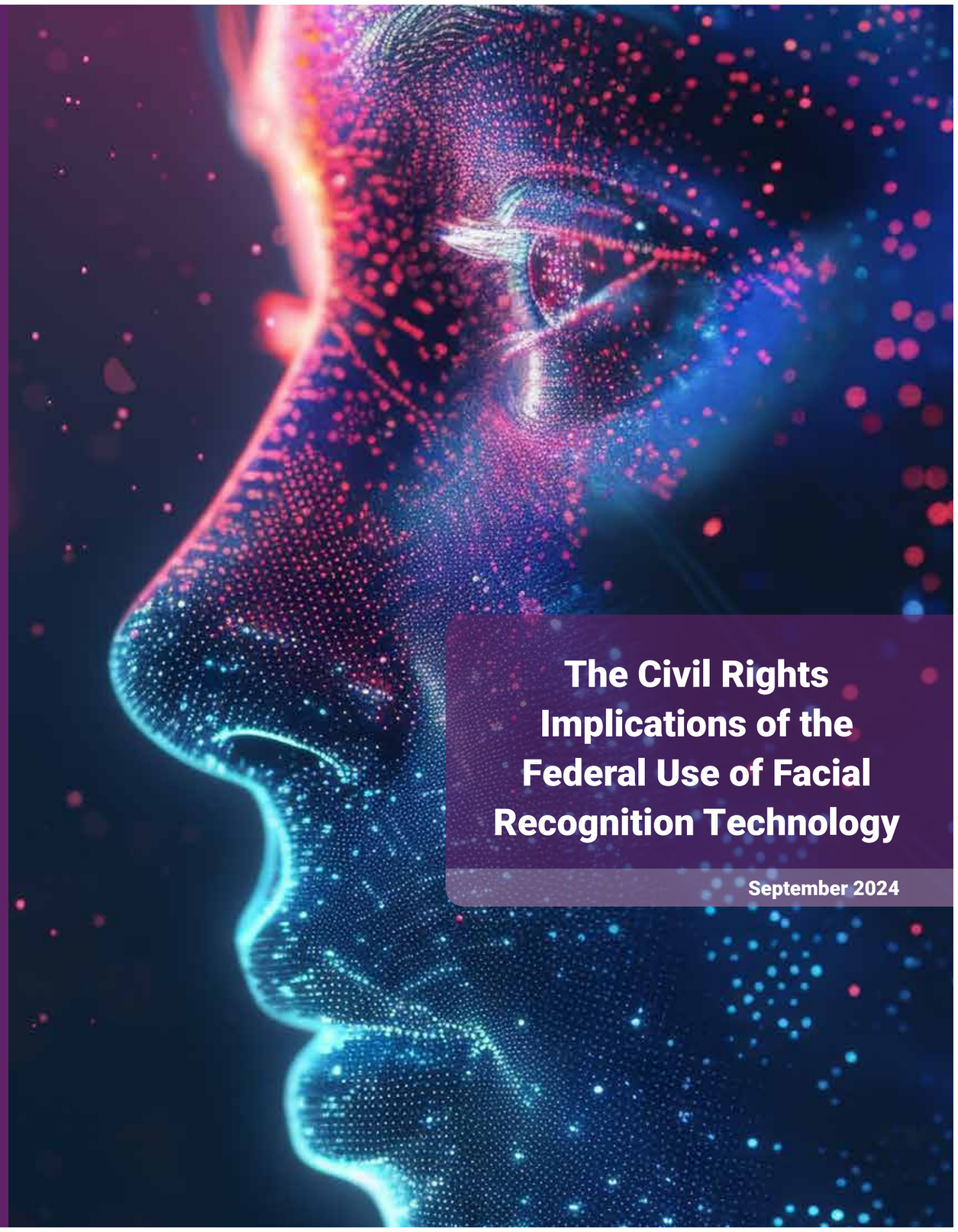
U.S. COMMISSION ON CIVIL RIGHTS

Washington, DC 20425
Official Business
Penalty for Private Use $300

Visit us on the Web: www.usccr.gov

The Civil Rights Implications of the Federal Use of Facial Recognition Technology



The Civil Rights Implications of the Federal Use of Facial Recognition Technology

September 2024

U.S. COMMISSION ON CIVIL RIGHTS

The U.S. Commission on Civil Rights is an independent, bipartisan agency established by Congress in 1957. It is directed to:

- Investigate complaints alleging that citizens are being deprived of their right to vote by reason of their race, color, religion, sex, age, disability, or national origin, or by reason of fraudulent practices.
- Study and collect information relating to discrimination or a denial of equal protection of the laws under the Constitution because of race, color, religion, sex, age, disability, or national origin, or in the administration of justice.
- Appraise federal laws and policies with respect to discrimination or denial of equal protection of the laws because of race, color, religion, sex, age, disability, or national origin, or in the administration of justice.
- Serve as a national clearinghouse for information in respect to discrimination or denial of equal protection of the laws because of race, color, religion, sex, age, disability, or national origin.
- Submit reports, findings, and recommendations to the President and Congress.
- Issue public service announcements to discourage discrimination or denial of equal protection of the laws.[1]

MEMBERS OF THE COMMISSION

U.S. Commission on Civil Rights
1331 Pennsylvania Avenue, NW
Washington, DC 20425

(202) 376-8128 voice
TTY Relay: 711

www.usccr.gov

1 42 U.S.C. §1975a.

The Civil Rights Implications of the Federal Use of Facial Recognition Technology

United States Commission on Civil Rights
2024 Statutory Enforcement Report

UNITED STATES COMMISSION ON CIVIL RIGHTS

1331 Pennsylvania Ave., NW • Suite 1150 • Washington, DC 20425 www.usccr.gov

Letter of Transmittal

September 19, 2024

President Joseph R. Biden
Vice President Kamala Harris
Speaker of the House Mike Johnson
President Pro Tempore of the Senate Patty Murray

Dear President Biden, Vice President Harris, Speaker Johnson, and President Pro Tempore Murray,

On behalf of the United States Commission on Civil Rights ("the Commission"), I am pleased to transmit our briefing report, *The Civil Rights Implications of the Federal Use of Facial Recognition Technology.* The report is also available in full on the Commission's website at www.usccr.gov.

In response to the federal government's increasing use of facial recognition technology (FRT), the Commission examined three federal departments' use of the technology: the Department of Justice (DOJ), Department of Homeland Security (DHS), and the Department of Housing and Urban Development (HUD). The Commission's investigation included testimony from subject matter experts, including government officials, academics, researchers, software developers, and legal experts. The Commission also received several public comments, as well as interrogatory responses from the DOJ, DHS, and HUD. Finally, the Commission made a first-of-its-kind site visit to DHS' Maryland Test Facility (MdTF) to learn about industry-leading developments in the testing of FRT and other biometric artificial intelligence (AI).

The Commission majority approved key findings including the following: FRT is used by DOJ, DHS, and HUD, as well as their funding recipients, in several programs across the FBI, TSA, CBP, and public housing agencies (PHAs). There are currently no federal laws or regulations that expressly authorize or limit FRT use by the federal government, and as of July 2024, there is no official, standardized policy published for federal FRT use.

While DOJ and DHS recently adopted interim FRT policies, HUD does not track FRT use. For the DOJ, there is no comprehensive data available regarding the accuracy of the FRT that is used by law enforcement in its real-world application. Within DHS, CBP has implemented facial biometrics into the entry processes at all international airports and into the exit processes at 53 airports, as well as expanded facial biometrics at 40 seaports and all pedestrian lanes at the southwest and northern Border ports of entry. HUD is proliferating FRT use largely through its grant programs for PHAs, putting FRT in the hands of grantees with no regulation or oversight. If HUD is providing funds for FRT—which is known to have higher misidentification rates for minorities—in housing where

tenants are disproportionately female and people of color, issues relating to access, eviction, and other punishments could lead to Title VI violations.

With respect to FRT accuracy and bias, the National Institute of Standards and Technology (NIST) testing is voluntary and represents laboratory—not real-world—results. Thus, NIST cannot say that its evaluated programs are accurately representative of the performance of all FRT deployed throughout the country. Algorithmic accuracy rates can vary widely among developers, but even with the highest-performing algorithms, tests have shown there are likely to be false positives for certain demographic groups, specifically Black people (particularly Black women), people of East Asian descent, women, and older adults. A promising FRT testing model does exist: DHS, through its Science and Technology Directorate, funds FRT research, testing, and evaluation at MdTF, which specializes in "scenario testing" of the entire FRT system as it is intended to be deployed. DHS is the only agency known to be testing FRT in this way.

The Commission majority voted for key recommendations including the following:

Congress should direct and empower NIST to develop an operational testing protocol that agencies can use to assess how effective, equitable, and accurate their FRT systems are when actually deployed. They should also condition the receipt of federal funds by grantees on the adoption of national training standards for individuals who review and analyze the results returned by FRT. Furthermore, Congress should provide a statutory mechanism for legal redress by individuals harmed by misuse or abuse of FRT.

As Chief AI Officers (CAIOs) become established across agencies, they should develop and incentivize the adoption of national training standards for individuals who review and analyze the results returned by FRT algorithms. For FRT that is rights-impacting, CAIOs should enable 1) the assessment of FRT in a real-world context 2) mitigate disparities that lead to, or perpetuate, unlawful discrimination or harmful bias, and 3) consult affected communities for feedback to inform agency decision-making regarding FRT. CAIOs should also consult DHS' MdTF as a template for real-world FRT testing to ensure it will work in its intended contexts.

Any agency using FRT should have a publicly available use policy. If agencies do use FRT, they should audit their use to ensure it complies with government policy. FRT vendors providing the federal government with solutions should provide users with ongoing training, technical support, and software updates to ensure their systems can maintain high accuracy across demographic groups in real-world deployment contexts. Furthermore, agencies should ensure their CAIOs work in close coordination with existing responsible officials and organizations within their organizations, including Civil Rights and General Counsel offices, to advise and update agency FRT guidance, implementation, and oversight.

Federal grantees using FRT should provide verified results with respect to accuracy and performance across demographics from NIST's FRT Evaluation or similar government-validated third-party test.

We at the Commission are pleased to share our views, informed by careful research and investigation as well as civil rights expertise, to help ensure that all Americans enjoy civil rights protections to which we are entitled.

For the Commission,

Rochelle M. Garza

Table of Contents

Acknowledgements

This report was produced under the direction of and with the contribution of Dr. Marik Xavier-Brier, Director of the Commission's Office of Civil Rights Evaluation (OCRE). OCRE Social Scientist Dr. Julie Grieco performed principal research and writing.

Commissioners' Special Assistants Nathalie Demirdjian-Rivest, Alexis Fragosa, John Mashburn, Carissa Mulder, Thomas Simuel, Irena Vidulovic, Stephanie Wong, and Yvesner Zamar assisted their commissioners in reviewing the report.

Commissioner Legal Interns Audrey Miller, Juris Doctorate Candidate (Expected 2026), American University College of Law, Maximillian Mallet, B.A. Candidate (Expected 2024), Williams College, and Noorkaran Chima, B.S. Candidate (Expected 2026) also offered valuable research assistance.

The Commission's General Counsel David Ganz and Attorney-Advisors Sheryl Cozart and Pilar Velasquez McLaughlin and Legal Intern Molly Hill, Juris Doctorate Candidate (Expected 2026), American University Washington College of Law reviewed and approved the report for legal sufficiency.

[This page is left intentionally blank]

EXECUTIVE SUMMARY

Facial Recognition Technology (FRT) is a branch of Artificial Intelligence (AI) that has the capability, through the use of algorithms, to scan massive datasets of facial images to determine whether two images belong to the same person. FRT has several compelling use cases and has been adopted by federal agencies and law enforcement to aid in fulfilling their missions. The field of AI has advanced rapidly, and with increased testing and algorithm training, FRT capabilities continue to grow and improve. However, meaningful federal guidelines and oversight for responsible FRT use have lagged behind the application of this technology in real-world scenarios. While a robust debate exists surrounding the benefits and risks associated with the federal use of FRT, many agencies already employ the use of this technology. Even when used in good faith, when FRT is deployed in contexts connected to civil rights, an inaccurate or misused FRT result could lead to serious consequences, including wrongful arrest, unwarranted surveillance, or discrimination.[1]

With the advent of biometric technology and its widespread use by both private and government entities, the Commission studied how certain federal government agencies are utilizing this technology, specifically FRT, in compliance with existing civil rights laws. As more federal agencies expand their use of FRT, questions and concerns about the technology emerge, such as, how the technology is used and by whom, and how data are being shared, accessed, and stored. Additionally, the use of FRT by federal agencies has brought up concerns if the usage disproportionately impacts certain communities. As such, the Commission voted unanimously in December 2023 to investigate the federal usage of and role in regulating FRT. This report focuses specifically on three departments: U.S. Department of Justice (DOJ), U.S. Department of Homeland Security (DHS), and U.S. Department of Housing and Urban Development (HUD). The report explores how FRT is being utilized by these agencies, the prevalence of training (or lack thereof) these Departments have in place, the emerging civil rights concerns regarding FRT usage, and steps the respective Departments are taking to mitigate these concerns.

There are several laws that prohibit discrimination and protect the civil rights and civil liberties of persons in the United States, including laws that protect against discrimination with regard to FRT.[2] Similarly, the Privacy Act of 1974, as amended, 5 U.S.C. § 552a, provides Americans with protections regarding the collection, storage, and use of personal information that may constrain or limit the use of FRT by federal agencies.[3] However, as of the writing of this report, there are no laws

[1] *See infra* section Civil Rights Concerns.

[2] Pursuant to 6 U.S.C. § 345 and 42 U.S.C. § 2000ee-1, the U.S. Department of Homeland Security CRCL is charged with investigating and assessing complaints against DHS employees and officials of abuses of civil rights, civil liberties, and profiling on the basis of race, ethnicity, or religion. See 6 U.S.C. § 345 and 42 U.S.C. § 2000ee-1. This includes reviewing complaints related to facial recognition technology. *See also* Titles IV, VI, VII of the Civil Rights Act. Additionally, several government agencies have joined to develop standards for AI with the publication of A Joint Statement on Enforcement of Civil Rights, Fair Competition, Consumer Protection, and Equal Opportunity Laws in Automated Systems, available at: https://www.justice.gov/crt/media/1346821/dl?inline (noting that "[e]xisting legal authorities apply to the use of automated systems and innovative new technologies just as they apply to other practices.").

[3] Additionally, the Federal Information Modernization act of 2014 requires that agencies and their contractors maintain programs that provide adequate security for all information collected, processed, transmitted, stored, or disseminated in

that expressly regulate the use of FRT or other AI by the federal government, and no constitutional provisions governing its use. There are also no federal regulations specifically protecting individual civil rights in the course of federal government use of FRT or other AI technology and no provisions requiring regular oversight of the government use of such technologies.[4]

One significant concern regarding the usage of FRT centers on privacy. FRT's potential for surveillance and covert use, paired with the widespread availability of personal information that can be associated with a facial image implicates privacy concerns. The lack of transparency and regulation raises privacy concerns due to the technology's collection and storage of personal and biometric information. Images of faces, as with other biometric systems, can be used for surveillance purposes without a person's knowledge or consent.[5]

Other civil rights concerns have emerged due to widespread FRT use. First, the technology's relatively easy development and ability for inexperienced and inadequately trained operators to wield makes its use easy to expand without fully understanding its capabilities and risks. Additionally, the observed differences in false positive and false negative match rates[6] across phenotypes and demographic groups raise discrimination and equal protection concerns.[7] As this report discusses, FRT has become a useful tool for both law enforcement and homeland security purposes. Therefore finding a balance between safeguarding Americans' civil rights and the use of this technology remains of critical importance.

A central concern surrounding FRT use is the accuracy of FRT systems (i.e., the combination of the algorithm with hardware, such as cameras). Algorithmic accuracy rates can vary widely among developers and can result in false positive and false negative matches. Fluctuating accuracy rates can lead to discriminatory practices and potentially violate an individual's civil rights. False positive demographic differentials (i.e., inaccurately attributing a photo of two different people as the same person) are larger than those related to false negatives (i.e., failure to match two images of one person as the same person) and exist broadly across many, but not all, algorithms.[8] It should be noted that false positives and false negative rates are determined by a cutoff threshold set for the algorithm by the user, and this threshold will often vary depending on the intended use for the FRT algorithm.[9]

---

general support systems and major applications. *See* Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014) (codified at 44 U.S.C. §§ 3551–3558). Similarly, the Aviation and Transportation Security Act, Pub. L. 107–71, Nov. 19, 2001, 115 Stat. 597, at sec. 106, permits the use of biometrics for airport perimeter screening, secured-area access control, and pilots.

[4] *See, infra* section Legal Background and Framework.

[5] *See* American Civil Liberties Union, "Face Recognition Technology," https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology (accessed Mar. 25, 2024).

[6] A false positive result occurs when a system inaccurately recognizes a photo of two different people as the same person. Conversely, a false negative result occurs when a system fails to match two images of one person as the same person. *See*, National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,* Dec. 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[7] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.

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

[9] *See, infra* note 167.

For example, the threshold to unlock a smartphone is set high to prevent unauthorized access, and a user can enter a password if the FRT fails; yet airport security FRT thresholds would be set low for the sake of public safety, and a security agent can check the results against other information.[10]

One way to test for accuracy is for FRT developers to submit their algorithms to the National Institute of Standards and Technology (NIST), which conducts evaluations that measure the core algorithmic capabilities of biometric recognition technologies and reports accuracy, reliability, and sensitivity of algorithms.[11] NIST biometric evaluations advance the technology by identifying and reporting gaps as well as current limitations of biometric recognition technologies.[12]

NIST testing has found that across different demographics, false positive differentials[13] can vary by factors of 10 to beyond 100, depending on the algorithm. Put differently, these rates mean that some demographics can be 10 times or beyond 100 times more likely to be misidentified, depending on the algorithm being tested. False negatives tend to be more algorithm-specific and vary often by factors below three.[14] Regarding race, there are higher false positive rates for Black people and people of East Asian descent relative to those of White people.[15] Additionally, there are higher false positive rates for women (compared to men) and the elderly (compared to middle-aged adults).[16] These effects apply to most algorithms, including those developed in the United States and Europe.[17] These differentials are smaller or undetectable with high-performing algorithms in certain applications.[18]

Additionally, FRT human reviewers are not immune from "automation bias," the propensity for humans to favor suggestions from automated decision-making systems and to ignore or fail to seek out contradictory information made without automation.[19] These findings are significant for a host of reasons: false negative results can threaten national security or public safety, and false positive results can lead to an individual being unlawfully detained or arrested.[20]

---

[10] Example provided by DOJ Affected Agency Review, Jun. 21, 2024.
[11] Patrick Grother, Computer Scientist, Information Technology Laboratory, National Institute of Standards and Technology (NIST), Written Statement for the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, at (hereinafter Grother Statement).
[12] Grother Statement, at 4.
[13] A differential means that an algorithm's ability to match two images of the same person varies from one demographic group to another. National Institute of Standards and Technology, "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.
[14] National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,* Dec. 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[15] Grother Statement, at 6.
[16] Ibid.
[17] Ibid.
[18] National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,* Dec. 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[19] OMB Draft Guidance on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence https://www.whitehouse.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-draft-for-public-review.pdf.
[20] There have been seven confirmed cases of misidentification due to the use of facial recognition technology.

While FRT can assist in criminal investigations, its accuracy rates can be concerning, particularly with respect to match rate differentials for people of color. Additionally, the use of FRT may raise concerns regarding disclosure of FRT use to defense attorneys.[21] As a 2022 report from the Georgetown Law Center on Privacy & Technology outlines: "While law enforcement officials, face recognition companies and others speak about face recognition as an investigative lead only, in the absence of caselaw or other guidance, it has in some cases been the primary, if not the only, piece of evidence linking an individual to the crime."[22] That said, FRT use among law enforcement agencies and public defenders as a tool for investigations and exonerations grows with the technology's advancement.[23]

Civil rights and privacy advocates also point out that there is no comprehensive data available regarding the accuracy of the FRT that is used by law enforcement in its real-world application. For instance, there are no publicly available or standardized tests for the images used by law enforcement FRT systems, such as low-resolution or grainy images from sources such as closed-circuit television (CCTV) cameras.[24] There are also no data to show how often police facial recognition searches are accurate.[25] The accuracy of eyewitness identifications, which are a contributing factor in wrongful convictions,[26] is also something the criminal justice system lacks data on with the exception of overturned convictions. FRT results may be more accurate than eyewitnesses; nonetheless, more widespread data demonstrating effectiveness would be beneficial. Importantly, when FRT is deployed by the criminal justice system to effect an arrest, possible technological support errors are not mere data points worthy of anecdotal study; they could impact real people "whose lives are

---

See Alyxaundria Sanford, "Artificial Intelligence Is Putting Innocent People at Risk of Being Incarcerated," *Innocence Project,* Feb.14, 2024, https://innocenceproject.org/artificial-intelligence-is-putting-innocent-people-at-risk-of-being-incarcerated/.

[21] Clare Garvie, Fourth Amendment Center Training and Resource Counsel, National Association of Criminal Defense Lawyers (NACDL), testimony, *Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing Before the U.S. Comm'n on Civil Rights, Washington, DC*, Mar. 8, 202, transcript, p. 207 (hereinafter cited as *Facial Recognition Technology Briefing*).

[22] Georgetown Law Center on Privacy & Technology, *A Forensic Without The Science: Face Recognition In U.S. Criminal Investigations,* Dec. 6, 2022, https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/.
It should be noted that DHS does have guidance stating "FR technologies used for identification may not be used as the sole basis for law or civil enforcement related actions, especially when used as investigative leads. Any potential matches or results from the use of FR technology for identification are manually reviewed by human face examiners prior to any law or civil enforcement action." DHS Affected Agency Review, Jun. 28, 2024.

[23] Ton-That Statement, at 1; Kashmir Hill, "Clearview AI, Used by Police to Find Criminals, Is Now in Public Defenders' Hands," *The New York Times,* Sep. 18, 2022, https://www.nytimes.com/2022/09/18/technology/facial-recognition-clearview-ai.html..

[24] Katie Kinsey, Chief of Staff, NYU School of Law Policing Project, Written Statement for the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, at 3 (hereinafter Kinsey Statement).

[25] Clare Garvie, Fourth Amendment Center Training and Resource Counsel, National Association of Criminal Defense Lawyers (NACDL), Written Statement for the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, at 5 (hereinafter Garvie Statement).

[26] Innocence Project, "Eyewitness Misidentification," https://innocenceproject.org/eyewitness-misidentification/ (accessed May 22, 2024).

irreparably harmed by a wrongful arrest."[27] This is not unique to the use of FRT but raises concerns regarding how quickly the technology is being deployed in the real world.

President Biden issued Executive Order 14074 in May 2022 intended, in part, to safeguard the use of FRT and other sophisticated algorithmic tools.[28] The order directed DOJ to contract with the National Academy of Sciences (NAS) to conduct a study on FRT and other technologies using biometric information, and publish a report detailing the findings of that study, as well as any recommendations or guidance relating to the federal government's use of FRT.[29] In January 2024, the NAS published its report,[30] and many of its recommendations are discussed in Chapter 3 of this report. In addition to President Biden's Executive Order, members of Congress have introduced legislation addressing FRT, including bills that would limit FRT's use by law enforcement agencies,[31] prohibit the use of FRT and other biometric recognition technology in most federally funded public housing,[32] and repeal existing authorization for the Transportation Security Administration (TSA) to use FRT.[33]

During the Commission's briefing, NIST representatives and other experts testified that algorithm testing alone is not sufficient to account for the entire system at work.[34] In response to this testimony, a bipartisan subcommittee from the Commission conducted a first of its kind site visit to DHS's Maryland Test Facility (MdTF), which was opened in 2014 to support DHS's Science and Technology Directorate (S&T). MdTF is a 24,000 square foot laboratory space fully instrumented and designed for scenario and operational testing[35] of biometric systems using human subjects.[36] MdTF's FRT testing, explained further in Chapter 2, is distinct from NIST's in that it specializes in scenario testing and full-system demonstrations of FRT as it is intended to be utilized in real-world scenarios,[37] whereas NIST testing focuses solely on algorithmic testing. While algorithm testing

---

[27] Garvie Statement, at 5.
[28] The White House, *FACT SHEET: President Biden to Sign Historic Executive order to Advance Effective, Accountable Policing and Strengthen Public Safety* (May 25, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/25/fact-sheet-president-biden-to-sign-historic-executive-order-to-advance-effective-accountable-policing-and-strengthen-public-safety/.
[29] Exec. Order No. 14074, *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety*, May 25, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/05/25/executive-order-on-advancing-effective-accountable-policing-and-criminal-justice-practices-to-enhance-public-trust-and-public-safety/
[30] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.
[31] *See, infra* notes 627-635; 634-635.
[32] *See, infra* notes 634-635.
[33] *See, infra* notes 644-646. This attempt was unsuccessful.
[34] Grother Statement, at 7; Georgetown Law Center on Privacy & Technology, *A Forensic Without The Science: Face Recognition in U.S. Criminal Investigations,* Dec. 6, 2022, https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/
[35] Scenario testing gathers biometric samples, and assesses the full biometric system, essentially testing how the technology performs within its intended use. Operational testing tests a technology in its actual location. *See, infra* note 469.
[36] Vemury Statement, at 1.
[37] S&T Directorate MdTF Presentation.

targets the algorithm itself for accuracy, scenario testing tests FRT in simulated use cases to mimic real world operational application of the entire FRT system.[38]

As of the writing of this report, DHS is the only agency known to be testing FRT and other biometric AI in this way. The MdTF lab was created not only to test, but also to engage the industry and educate AI stakeholders on the current state and challenges of biometric technology.[39] However, despite being open since 2014, the center has not had engagement from members of Congress, and limited engagement from other federal agencies, which made the Commission's visit unique. During its visit, the Commission learned about some of the challenges posed by FRT, including the significant impact on accuracy that can result from the equipment being used (e.g., camera, webcam, smartphone). This kind of testing sheds much needed light on FRT's efficiency, effectiveness, and equitability when deployed in real-world scenarios with human subjects of different races, genders, and skin tones.

This report analyzes publicly available studies and data and synthesizes reliable research and evidence regarding federal agency utilization of FRT. This report also surveys the government's efforts to enforce existing civil rights laws as they apply to federal, state, and local use of FRT and responses to allegations of civil rights violations. In addition, the Commission held a public briefing on March 8, 2024, to receive written and oral testimony from academics and researchers, legal experts, current government officials, and civil rights advocates. The Departments of Justice, Homeland Security, and Housing and Urban Development were invited to participate in the briefing and provide oral and written testimony, however, only DHS agreed to do both. Following the briefing, DOJ and HUD submitted written testimony for the record. The Commission also sent formal requests for information to the three departments. All three departments responded to the Commission's requests, and the information provided is found herein.

Within DOJ, FRT is primarily utilized by the Federal Bureau of Investigations (FBI) and the U.S. Marshals Service (USMS), most often to generate leads in criminal investigations and during efforts to locate known subjects. Images that are submitted to the Criminal Justice Information Services (CJIS) systems by law enforcement, known as "probe photos," can be obtained from prior booking photos (e.g., arrest photos), driver's licenses, public social media accounts, public websites, cell phones, CCTV still images, electronic surveillance, and photos maintained by law enforcement partners.[40]

DOJ announced the Department's interim FRT policy in December 2023. It "prohibits unlawful use of FRT, provides guardrails to ensure effective and compliant use, and addresses the Department's FRT governance structure, including scope of FRT use, implementation, procurement, training, protection of privacy and civil rights, accuracy, the approval process for FRT use, accounting and reporting, and data retention."[41] The policy also requires that systems be assessed for accuracy across

[38] Ibid.
[39] Ibid.
[40] U.S. Dep't of Justice, DOJ Responses to U.S. Commission on Civil Rights Interrogatories, Mar. 26, 2024.
[41] DOJ Statement, at 2.

demographic groups, that personnel using or approving FRT receive training, and that activity protected by the First Amendment not be the sole basis for the use of FRT.[42]

The DOJ interim FRT policy also prohibits the use of FRT results as a means of positive identification or as the sole basis for an arrest.[43] The interim policy states that FRT results are intended only to generate investigative leads that require additional investigation to substantiate or invalidate those leads.[44] The policy states that FRT results standing alone may not serve as the sole basis on which Department personnel apply for search and/or arrest warrants or secure complaints/indictments.[45] The DOJ explained to the Commission that FRT results may be used in conjunction with other factors discovered in an investigation, and that federal prosecutors bear the exclusive responsibility for decisions such as issuing subpoenas, obtaining search and arrest warrants, and determining the sufficiency of evidence to establish probable cause. They also decide when, whom, how, and whether to prosecute.[46]

However, while experts at the Commission's March briefing affirmed the DOJ's policy limiting the use of FRT for investigative leads only, there is insufficient data to confirm adherence to this rule in practice.[47] There are no publicly available databases indicating the frequency of departmental FRT searches on individuals, the demographics of the individuals subject to a search, the types of crimes, and the accuracy of any results. Therefore, conducting public oversight of the government's use of FRT to determine if civil rights violations are occurring is extraordinarily difficult.[48]

DHS uses biometrics (such as fingerprints, iris, and face recognition) to help enable operational missions, both to support national security and public safety, and deliver benefits and services with greater efficiency and accuracy.[49] DHS uses face recognition to (a) detect and identify fraud and support cross-border criminal investigations; and (b) enhance the delivery of benefits and services, like expediting verification of travelers' identities. DHS has several components that employ facial recognition technology in their operations, including the Office of Biometric Identity Management (OBIM), U.S. Customs and Border Protection (CBP), Office of Intelligence and Analysis (I&A), U.S. Citizenship and Immigration Services (UCSIS), U.S. Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), and U.S. Secret Service (USSS).[50]

DHS's Office of Civil Rights and Civil Liberties (CRCL) Deputy Officer for Programs and Compliance, Peter Mina, testified at the Commission's briefing that "DHS uses biometrics such as fingerprints, iris and face recognition to enable operational missions, both to support national

[42] DOJ Statement, at 2-3.
[43] DOJ Statement, at 6.
[44] Ibid.
[45] DOJ Affected Agency Review, Jun. 21, 2024.
[46] Ibid.
[47] Garvie Testimony, p. 235.
[48] Kinsey Statement, at 4.
[49] U.S. Dep't of Homeland Security, DHS Responses to U.S. Commission on Civil Rights Interrogatories, Apr. 17, 2024, at 2.
[50] Ibid., at 2-3.

security and public safety and deliver benefits and services with greater efficiency and accuracy."[51] In September 2023, DHS issued its Facial Recognition and Face Capture Directive on FRT usage which outlines the authorized usage of the technology for the entire Department.[52] Given DHS' broad scope and mission, several agencies housed within the Department utilize FRT and have established their own protocols, but are still governed by the Directive. While a discussion of all of DHS' agencies and their usage of FRT is beyond the purview of this report, the Commission focuses on CRCL's role in addressing civil rights concerns, as well as on CBP, TSA, and ICE.

CRCL asserts that DHS issued the Facial Recognition and Face Capture Directive to ensure that the technology is being implemented and deployed responsibly and that the agency is "proactively assessing" the utilization of this technology.[53] DHS also has a Science & Technology Directorate (S&T) that researches and tests AI technology; S&T's results are shared across DHS components and offices regarding the technology's performance, and exist to help procurers better understand how to specify relevant metrics and performance benchmarks when purchasing these technologies.[54] The Commission also received testimony from DHS regarding its work toward developing a new international standard on evaluating biometric systems for demographic differentials, and other standardization efforts relevant to facial recognition, such as how to handle different levels of facial image quality.[55]

Regarding HUD, the Commission's research shows that FRT is integrated into surveillance cameras used in federally funded public housing programs.[56] HUD wrote to the Commission stating that it does not require its public housing agency (PHA) grantees to implement specific policies on FRT and does not keep a list of PHAs that elect to use FRT.[57] HUD also indicated that its funds provide program participants the "flexibility to purchase solutions and make investments that will provide decent, safe, and sanitary housing for residents."[58] The first time HUD mentioned FRT in its grant

[51] Peter Mina, Deputy Officer for Programs and Compliance, Civil Rights and Civil Liberties, U.S. Dep't of Homeland Security, testimony, *Facial Recognition Technology Briefing*, p. 86.
[52] U.S. Dep't of Homeland Security, "Use of Face Recognition and Face Capture Technologies," Sept. 11, 2023, https://www.dhs.gov/sites/default/files/2023-09/23_0913_mgmt_026-11-use-face-recognition-face-capture-technologies.pdf.
[53] Mina Testimony, pp. 87-88.
[54] Arun Vemury, Senior Engineering Advisor for Biometric and Identity Technologies, DHS Science and Technology Directorate, Written Statement for the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, at 3 (hereinafter Vemury Statement).
[55] Ibid.
[56] *See e.g.*, Michelle Ewert, Director, Washburn Law Clinic, Washburn University School of Law, Written Statement for the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, at 1 (hereinafter Ewert Statement); Douglas MacMillian, "Eyes on the poor: Cameras, facial recognition watch over public housing," *The Washington Post*, May 16, 2023, https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/; Lisa Desjardins and Andrew Corkery, "How surveillance camera are being used to punish public housing residents," PBS News, June 4, 2023, https://www.pbs.org/newshour/show/how-surveillance-cameras-are-being-used-to-punish-public-housing-residents; Rep. Maxine Waters and Rep. Ayanna Pressley, Letter to HUD Secretary Marcia L. Fudge, May 25, 2023, https://democrats-financialservices.house.gov/uploadedfiles/cmw_letter_hud_surveillance_tech_5.25.23_signed.pdf.
[57] U.S. Dep't of Housing and Urban Development, Response to USCCR Interrogatories.
[58] Ibid.

notices[59] was in April 2023, when HUD issued a notice indicating that its Emergency Safety and Security grant (ESSG) funds may not be used to purchase "automated surveillance and facial recognition technology."[60] Notably, this restriction applies only to *future* recipients of ESSG funds and does not limit use of surveillance tools by grantees that have already purchased them.[61]

The Commission heard testimony about property management companies employing access control technologies integrated with FRT.[62] Considering the potential inaccuracies of FRT relating to race, gender, and age discussed above, the use of access control technologies with FRT without oversight is especially problematic in subsidized housing, where tenants are "disproportionately women, disproportionately people of color and disproportionately seniors."[63]

There is no comprehensive data available regarding the purchasing of FRT by PHAs, and since HUD does not track or monitor FRT purchases via federal funds, it is difficult to determine how often these funds are being used for purposes of eviction. However, if FRT is being used to evict tenants in a discriminatory manner or has a disproportionate impact on people of color, this practice could also be a violation of Title VI of the Civil Rights Act of 1964, which HUD grantees must comply with.

The January 2024 NAS report recommended that the federal government take prompt action to sustain a vigorous program of FRT testing and evaluation, establish industry-wide standards, and form multi-disciplinary working groups to develop and periodically review standards for reasonable and equitable use.[64] The report also recommended that DOJ and DHS establish an FRT working group charged with developing "[m]inimum technical requirements for FRT procured by law enforcement agencies and a process for periodically evaluating and updating such standards."[65]

The NAS report also recommended policies and procedures to address local law enforcement failures to adhere to procedures and attain appropriate certification, and to establish mechanisms for redress by individuals harmed by FRT misuse or abuse.[66] It recommended that institutions developing or deploying FRT should take steps to cultivate greater community trust by adopting more inclusive designs and engaging with communities to help individuals understand FRT's capabilities,

---

[59] There is no mention of facial recognition technology in prior years of HUD ESSG notices. U.S. Dep't of Housing and Urban Development, "Notice PIH 2022-05," Mar. 10, 2022, https://www.hud.gov/sites/dfiles/PIH/documents/PIH2022-05.pdf; U.S. Dep't of Housing and Urban Development, "Notice PIH 2020-05," Sep. 17, 2020, https://www.hud.gov/sites/dfiles/PIH/documents/2020-25pihn.pdf; U.S. Dep't of Housing and Urban Development, "Notice PIH 2019-22," Aug. 19, 2019, https://www.hud.gov/sites/dfiles/PIH/documents/PIH-2019-22.pdf.

[60] U.S. Dep't of Housing and Urban Development, "Notice PIH 2023-10," Apr. 21, 2023, https://www.hud.gov/sites/dfiles/PIH/documents/2023PIH10.pdf.

[61] Douglas MacMillan, "Eyes on the poor: Cameras, facial recognition watch over public housing," *The Washington Post,* May 16, 2023, https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/.

[62] *See, infra* notes 531, 543-545.

[63] Michelle Ewert, Director, Washburn Law Clinic, Washburn University School of Law, testimony, *Facial Recognition Technology Briefing,* p.42.

[64] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.

[65] Ibid.

[66] Ibid.

limitations, and risks.[67] The report further suggested that the government develop requirements for the training and certification of officers and staff using FRT.[68] However, many researchers and civil rights advocates caution that merely setting standards will not be sufficient, and the federal government needs to actively ensure that FRT is being used responsibly and does not infringe upon Americans' civil rights.[69]

Chapter 1 of this report provides a brief introduction to AI and FRT, covers the legal frameworks implicated in the federal government's use of FRT, and concludes with a discussion of civil rights concerns. Chapter 2 discusses how DOJ, DHS, and HUD utilize FRT, the civil rights concerns surrounding its usage, and the respective efforts the departments are taking to address civil rights violations. Chapter 3 concludes the report with an analysis of efforts to develop guidelines and best practices in the utilization of FRT.

[67] Ibid.
[68] Ibid.
[69] *See* Brian Finch, Attorney, Pillsbury Winthrop Shaw Pittman LLP, testimony, *Facial Recognition Technology Briefing;* Heather Roff, Associate Fellow, Leverhulme Centre for the Future of Intelligence, University of Cambridge & Senior Research Scientists, Center for Naval Analysis, testimony*, Facial Recognition Technology Briefing.*

CHAPTER 1: Introduction to Artificial Intelligence and Civil Rights Protections

The definition of artificial intelligence largely depends on which field or discipline is doing the defining.[70] John McCarthy, a founder of the AI discipline, explained that AI is the science and engineering behind making intelligent machines. However, these machines are not confined to learning through mechanisms which are biologically observable.[71]

The first evolution of AI was witnessed from 1957 to 1974, when AI advanced as computers were able to store more information and became faster and more accessible.[72] However, due to the limited computational power of early computers, AI advancement was limited until the late 1990s and 2000s. One famous moment that gained worldwide attention was the advancement of machine learning,[73] which occurred in 1997 when the reigning chess champion and grand master Garry Kasparov was defeated by IBM's computer "Deep Blue."[74] That same year, *Dragon Systems* released the first publicly available speech recognition software for the Windows operating system, which was a significant step forward in machine learning capabilities.[75] The use of AI continued to spread throughout the late 90s and into the new millennium as larger computer hardware systems allowing for more computing power became widely available to consumers. Meanwhile, in the 2000s, AI research expanded into new arenas such as natural language processing[76] and robotics, which led the way to today's AI revolution.

In modern times, the definition of AI has become more refined.[77] AI is the science of machines learning from experience, adjusting to new inputs, and performing human-like tasks.[78] Branches of

---

[70] *See* Boris Kontsevoi, "What Exactly Is Artificial Intelligence? (Hint: It's All About The Datasets), Forbes, May 4, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/05/04/what-exactly-is-artificial-intelligence-hint-its-all-about-the-datasets/?sh=3b124d741bc9.

[71] John McCarthy, "What is Artificial Intelligence?" Computer Science Department, Stanford University, Nov. 12, 2007, https://www-formal.stanford.edu/jmc/whatisai.pdf.

[72] *See e.g.,* Rockwell Anyoha, "The History of Artificial Intelligence," Harvard University, Kenneth C. Griffin Graduate School of Arts and Sciences, Aug. 28, 2017, https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/.

[73] Machine learning and AI are often used interchangeably, but machine learning is one of the branches of AI and specifically refers to "the technologies and algorithms that enable systems to identify patterns, make decisions, and improve themselves through experience and data." *See e.g.,* Columbia Engineering, "Artificial Technology (AI) vs. Machine Learning, https://ai.engineering.columbia.edu/ai-vs-machine-learning/.

[74] Rockwell Anyoha, "The History of Artificial Intelligence," Harvard University, Kenneth C. Griffin Graduate School of Arts and Sciences, Aug. 28, 2017, https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/.

[75] Ibid.

[76] Natural language processing (NLP) is an interdisciplinary field of research that explores how computers can be used to understand and manipulate language text or speech (e.g., voice-activated digital assistants on smartphones, translation applications that decipher foreign languages). *See e.g.*, Gobinda G. Chowdhury, "Natural Language Processing," *Annual Review of Information Science and Technology*, vol. 37, (2003), https://pureportal.strath.ac.uk/files/131112/strathprints002611.pdf.

[77] Boris Kontsevoi, "What Exactly Is Artificial Intelligence? (Hint: It's All About The Datasets), Forbes, May 4, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/05/04/what-exactly-is-artificial-intelligence-hint-its-all-about-the-datasets/?sh=3b124d741bc9.

[78] "Artificial Intelligence: What it is and why it matters," *SAS,* https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html#:~:text=Artificial%20intelligence%20(AI)%20makes%20it,learning%20and%20natural%20language%20processing (accessed Dec. 19, 2023).

AI include logical AI, search programs, pattern recognition, representation, inference, commonsense knowledge and reasoning, learning from experience, planning, epistemology, ontology, heuristics, and genetic programming.[79] The federal government now defines artificial intelligence as:

> A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to – perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.[80]

The usage of AI technology has also expanded. AI was once confined to researchers but is now ubiquitous and used in a variety of ways by the public. For instance, people use it to plan gardens, workouts, and meals; write speeches and emails; quickly skim academic articles and sort through archival pictures; transcribe clinical notes; assist in learning a new language and provide translation for travelers; and fix bugs in algorithmic codes.[81] One of the most commonly used aspects of machine learning is the predictive text that is built into word processing systems (e.g., Microsoft Word) and short message services (SMS), better known as cell phone texting. Predictive text systems can suggest words or even finish sentences for writers using natural language processing.[82]

Many AI systems work by combining large sets of data with intelligent, iterative processing algorithms to learn from patterns and features in the data they analyze.[83] Each time an AI system runs a round of data processing, it tests and measures its own performance and develops additional expertise.[84] The most basic part of AI is datasets. According to Boris Kontsevoi, President and CEO of Intetics Inc., a custom software development company, "[e]verybody is talking about AI and AI applications but a few are focusing on how accurate the data is and if the data is correct. Data collection needs to be deliberate—the success of its intended application depends on it."[85]

According to a McKinsey Global Institute study, nations that promote open data sources and data sharing are the ones most likely to see AI advances.[86] The Brookings Institute points out that the U.S. currently does not have a coherent national data strategy when it comes to the use of AI,[87] despite a recent Executive Order instructing the development of guidelines and best practices for AI

---

[79] John McCarthy, "What is Artificial Intelligence?" Computer Science Department, Stanford University, Nov. 12, 2007, https://www-formal.stanford.edu/jmc/whatisai.pdf.
[80] 15 U.S.C. § 9401(3).
[81] Francesca Paris and Larry Buchanan, "35 Ways Real People Are Using A.I. Right Now," *The New York Times,* Apr. 14, 2023, https://www.nytimes.com/interactive/2023/04/14/upshot/up-ai-uses.html.
[82] Anne McCarthy, "How 'smart' email could change the way we talk," *BBC,* Feb. 28, 2022, https://www.bbc.com/future/article/20190812-how-ai-powered-predictive-text-affects-your-brain.
[83] CSU Global, "How Does AI Actually Work?" Aug. 9, 2021, https://csuglobal.edu/blog/how-does-ai-actually-work.
[84] Ibid.
[85] Boris Kontsevoi, "What Exactly Is Artificial Intelligence? (Hint: It's All About The Datasets), *Forbes,* May 4, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/05/04/what-exactly-is-artificial-intelligence-hint-its-all-about-the-datasets/?sh=3b124d741bc9.
[86] Darrell M. West and John R. Allen, "How artificial intelligence is transforming the world," *Brookings,* Apr. 24, 2018, https://www.brookings.edu/articles/how-artificial-intelligence-is-transforming-the-world/.
[87] Ibid.

safety and security.[88] Currently, there are few protocols in place for promoting research access or platforms that make it possible to gain new insights from proprietary data.[89] At the same time, it is not always clear who owns the data or how much belongs in the public sphere.[90] This lack of transparency is a central theme when it comes to apprehension about the advancement of AI. Andrew Burt of Immuta, a data security platform and software company, stated:

> The key problem confronting predictive analytics is really transparency. We're in a world where data science operations are taking on increasingly important tasks, and the only thing holding them back is going to be how well the data scientists who train the models can explain what it is their models are doing.[91]

The concerns surrounding the expansion of AI are an important conversation especially as these technologies continue to become more widespread. A full discussion of AI and these concerns are outside the purview of this report, but the development of these systems provide an important framework to understand the implementation of facial recognition technology (FRT). While FRT is utilized in both the private and public sphere, this report focuses specifically on the federal government's use of FRT and AI technology.

Facial Recognition Technology

Facial recognition technology (FRT) uses software to determine the similarity between two facial images.[92] Facial recognition should not be confused with facial characterization, which is the process of computer software classifying a single face according to gender, age, emotion, or other characteristics.[93] The former uses algorithms to compare similarities between two faces, whereas the latter uses algorithms to classify a single face. There may be emerging civil rights concerns regarding the use of facial characterization, such as using the technology to "detect" an individual's identity markers (e.g., race, ethnicity, and sexual orientation) or to profile individuals,[94] but this report examines the use of FRT as a source of identification specifically.

Facial recognition technology (FRT) works by transforming an image of a face into a numerical expression (or template) that can be used to compare the similarity of facial images.[95] By comparing the templates of different faces, it is possible to determine whether two given faces belong to the

---

[88] Exec Order No. 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,* Oct. 30, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.
[89] Darrell M. West and John R. Allen, "How artificial intelligence is transforming the world," *Brookings,* Apr. 24, 2018, https://www.brookings.edu/articles/how-artificial-intelligence-is-transforming-the-world/.
[90] Ibid.
[91] Eric Siegel, "Wise Practitioner – Predictive Analytics Interview Series: Andrew Burt at Immuta," *Machine Learning Times,* Jun. 14, 2017, https://www.predictiveanalyticsworld.com/machinelearningtimes/wise-practitioner-predictive-analytics-interview-series-andrew-burt-at-immuta6142017/8716/.
[92] William Crumpler and James A. Lewis, "How Does Facial Recognition Work?" *Center for Strategic and International Studies,* Jun. 10, 2021, https://www.csis.org/analysis/how-does-facial-recognition-work.
[93] Ibid.
[94] Ibid.
[95] Ibid.

same subject, similar to how one might compare fingerprint records.[96] The Center for Strategic and International Studies (CSIS) explains:

> Modern facial recognition developers use deep learning[97] to automate a process of trial and error that helps identify the best filters for reliably generating robust templates. Training these systems involves providing them with a series of "triplets"—collections of three face images where two of the faces belong to one person and the third belongs to someone else. The system turns each of the three images into a template and then compares their similarity. The system is given the goal of achieving the maximum similarity for the templates coming from the same subject and the minimum similarity for the templates coming from different subjects.[98]

Unlocking a smartphone with biometrics, such as facial identification, is an example of FRT that is used daily by many individuals. For instance, Apple's FaceID places 30,000 infrared dots on the face it is examining and captures an image, using machine learning algorithms to compare the scan of a face with stored data about a face to determine whether they are the same.[99] The degree of accuracy of facial recognition is contingent on many factors including, but not limited to, the algorithm being used, the quality of the images being compared, and the size of the search space.[100]

Electronic Frontier Foundation explained in a statement to the Commission:

> Face recognition technology may include all or some of the following steps: (1) probe photo capture (choosing or creating the photo of the face to be identified such as selecting the still capture from a video); (2) photo editing (altering or changing the probe photo); (3) creation of a facial template (creating a "face vector" with FRT software, which is a purportedly unique imprint of the face); (4) selecting comparison data (choosing a group or database of face photos for comparison to the probe photo); and (5) algorithmic search (attempting to use FRT software to match the probe photo facial template to facial templates of the photos in the comparison data set).[101]

For the purposes of this report, it is important to recognize and differentiate between two different uses of FRT: verification and identification. FRT verification, also known as one-to-one (1:1)

---

[96] Ibid.
[97] Deep learning is a form of machine learning that uses algorithms to build brain-like logical structures known as artificial neural networks to process data. These networks can then be used to mimic the learning process of the human brain. *See* Christian Janiesch, Patrick Zschech, and Kai Heinrich, "Machine Learning and deep learning," *Electronic Markets*, vol. 31, (2021), https://link.springer.com/article/10.1007/s12525-021-00475-2.
[98] William Crumpler and James A. Lewis, "How Does Facial Recognition Work?" *Center for Strategic and International Studies,* Jun. 10, 2021, https://www.csis.org/analysis/how-does-facial-recognition-work.
[99] Bernard Marr, "The 10 Best Examples of How AI Is Already Used In Our Everyday Life," *Forbes,* Dec. 16, 2019, https://www.forbes.com/sites/bernardmarr/2019/12/16/the-10-best-examples-of-how-ai-is-already-used-in-our-everyday-life/?sh=31c6f9c31171.
[100] William Crumpler and James A. Lewis, "How Does Facial Recognition Work?" *Center for Strategic and International Studies,* Jun. 10, 2021, https://www.csis.org/analysis/how-does-facial-recognition-work.
[101] Electronic Frontier Foundation, Public Comment, Apr. 5, 2024 [on file].

matching, uses technology to confirm whether a person is connected to a specific identity record[102]—such as the FaceID described above, or identity verification that happens at airport security. FRT identification, also known as one-to-many (1:N or 1:many) matching, is used to determine whether a record for an *unknown* individual exists in a larger database of known faces.[103] In policing, the most well-known example of 1:many matching is the use of FRT to generate a lineup of potential suspects based on images or footage of a crime.[104] It is important to note, however, that FRT identification does not necessarily provide any information about the person in question, but can provide tracking information. For example, a retail store could use FRT to track customers' in-store purchasing behaviors and new or returning customers, but not collect any biographical information such as the individuals' name, address, or purchasing history.[105]

FRT Developers

As FRT expands, the number of companies that develop the technology continues to grow. Companies are increasingly providing FRT to the federal government, leading the Government Accountability Office (GAO) to study commercial facial recognition services used by selected federal law enforcement agencies from October 2019 through March 2022.[106] GAO found that the seven agencies in the review reported using five different services: IntelCenter, Marinus Analytics, Thorn, Idemia, and Clearview AI.[107]

IntelCenter offers Terrorist Facial Recognition, a web-based service utilized by CBP that allows users to search photos against a gallery of over 2.4 million faces extracted from open-source terrorist data. Marinus Analytics offers Traffic Jam, a web-based service that uses images from the online commercial sex market to identify victims of human trafficking in the U.S. and abroad. Marinus Analytics is used by CBP and the FBI.[108] Thorn's Spotlight, which the FBI also uses, is a web-based service using images from the online commercial sex market to find exploited children and identify their traffickers in support of sex trafficking investigations.[109] Idemia provides TSA its PreCheck traveler pre-screening program, and has processed over 20 million enrollments as of February 2024.[110] Clearview AI is one of the more prominent commercial providers of FRT to law enforcement agencies. The system's backbone is a database of more than 10 billion images that

[102] William Crumpler and James A. Lewis, "How Does Facial Recognition Work?" *Center for Strategic and International Studies,* Jun. 10, 2021, https://www.csis.org/analysis/how-does-facial-recognition-work.
[103] Ibid.
[104] Ibid.
[105] Ibid.
[106] These agencies included: Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), U.S. Customs and Border Protection (CBP), Drug Enforcement Administration (DEA), Federal Bureau of Investigation (FBI), Homeland Security Investigations, U.S. Marshals Service, U.S. Secret Service. *See* U.S. Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties*, Sept. 2023, https://www.gao.gov/products/gao-23-105607.
[107] Ibid.
[108] U.S. Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties,* Sept. 2023, https://www.gao.gov/products/gao-23-105607.
[109] Ibid.
[110] Idemia North America, "TSA," https://na.idemia.com/tsa/ (accessed Feb. 15, 2024).

Clearview claims to have scraped from Facebook, YouTube, Venmo, and millions of other sites.[111] In 2023, GAO reported utilization of Clearview AI's services, over the period 2021 to 2023, by the FBI, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Drug Enforcement Administration (DEA), U.S. Marshals Service (USMS), Homeland Security Investigations (HSI), and U.S. Secret Service (USSS).[112] Officials with ATF, DEA, and Secret Service reported to GAO that as of April 2023 they had halted use of the service.[113] Since the GAO report was published, DOJ has indicated that FRT is only used by FBI, USMS, and the Child Exploitation and Obscenity Section of the Criminal Division.[114]

Legal Background and Framework

Although the Civil Rights Acts of 1957 and 1964 prohibit discrimination on the basis of race, religion, sex, color, national origin and disability in a variety of contexts, such as employment and public accommodation—discussed below in detail—there are currently no federal constitutional provisions or statutes that expressly authorize or limit the use of FRT or other AI by the federal government. There are also no federal laws that explicitly protect an individual's civil rights in the use of FRT or other AI technology by the government.

U.S. Constitution

The U.S. Constitution contains, not unsurprisingly, no provisions explicitly related to AI or FRT. The use of these technologies has, however, raised certain civil rights concerns regarding transparency and privacy. Although the focus of this report is the impact of FRT on civil rights, this section will briefly discuss Constitutionally guaranteed rights that may be negatively impacted if FRT is not utilized responsibly.

The Fourth Amendment is often associated with privacy from state intrusion in the form of "unreasonable" search and seizure.[115] FRT may implicate several protections under the Fourth Amendment umbrella, but scholars and case law are split on the topic. It is not clear whether a person has a reasonable expectation of privacy in a public setting,[116] if facial features are private under the

---

[111] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times,* Jan. 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; Will Knight, "Clearview AI Has New Tools to Identify You in Photos," *Wired,* Oct. 4, 2021, https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos/.
The 2020 NYT article states Clearview has more than 3 billion images, and the 2021 Wired article indicates Ton-That said they have more than 10 billion.

[112] U.S. Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties,* Sept. 2023, https://www.gao.gov/products/gao-23-105607.

[113] Ibid.

[114] U.S. Dep't of Justice, (Amended)Written Statement for the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Rec'd May 22, 2024, at 5 (hereinafter DOJ Statement).

[115] U.S. Const. amend. IV; *Mapp v. Ohio*, 367 U.S. 643, 655 (1961).

[116] "If an article is already in plain view, neither its observation nor its seizure would involve any invasion of privacy." *Horton v. California*, 496 U.S. 128, 133(1990) citing *Arizona v. Hicks,* 480 U.S. 321, 325, 107 S.Ct. 1149, 1152, 94

"plain view" doctrine, if the "third-party" doctrine prevents triggering the Fourth Amendment, and to what extent the government has access to GPS tracking data and for how long.[117]

The Fourth Amendment, importantly, governs state actors – limiting its potential protections.[118] In the 2018 case, *Carpenter v. United States*, the plaintiff alleged that the government violated his expectation of privacy in his physical location when the government accessed his historical cell-site records.[119] With this data, the FBI was able to map the plaintiff's whereabouts and create an "all-encompassing" record.[120] The Court suggested that the acquisition of time-stamped data from cell phone records that provide "an intimate window into a person's life" may constitute a search subject to Fourth Amendment scrutiny.[121] In a similar way, privacy concerns and other legal issues may emerge as social media and other third party databases compile photos captured by FRT that are then acquired by law enforcement.

While there is no explicit constitutional right to privacy, there are two major statutes that govern the collection and use of personal information by a federal agency: the Privacy Act of 1974 and the E-Government Act of 2002.[122] Neither act directly addresses FRT, however, they do place limits on how agencies collect, store, and use information directly and through partnerships with private parties and state and local government.[123]

The Confrontation Clause of the Sixth Amendment provides that the accused in a criminal prosecution shall have the right to confront and cross-examine witnesses.[124] In *Crawford v. Washington*, the Supreme Court held that out-of-court statements by witnesses that are testimonial are inadmissible unless witnesses are unavailable and defendants had prior opportunity to cross-examine witnesses.[125] However, "non-testimonial" statements not intended to be preserved as

---

L.Ed.2d 347 (1987); *Illinois v. Andreas,* 463 U.S. 765, 771, 103 S.Ct. 3319, 3324, 77 L.Ed.2d 1003 (1983);; *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 979 F.3d 219, 231 (4th Cir. 2020), ("Precedent suggests law enforcement can use security cameras without violating the Fourth Amendment."). *See* also National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance, pp. 71-72.

[117] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.

[118] U.S. Const. amend. IV.

[119] *Carpenter v. United States*, 585 U.S. 296, 311 (2018)

[120] *Id*.

[121] *Id.*; Cong. Rsch. Serv., R46541, Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations 15-16 (2020) https://crsreports.congress.gov/product/pdf/R/R46541.

[122] Privacy Impact Assessments ("PIAs") are required by Section 208 of the E-Government Act for all Federal government agencies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing information technology that manages information in identifiable form. DHS Affected Agency Review, Jun. 28 2024.

[123] *See* Candice N. Wright, "Facial Recognition Technology: Federal Agencies' Use and related Privacy Protections," U.S. Government Accountability Office, Testimony Before the Subcommittee on Investigations and Oversight, Committee on Science, Space, and Technology, June 29, 2022, https://www.gao.gov/assets/gao-22-106100.pdf.

[124] U.S. Const. amend. VI (noting that "in all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him;").

[125] 541 U.S. 36 (2004).

evidence are admissible and are not subject to cross-examination at trial.[126] In regards to FRT, there are some concerns that if results from an electronic search are used as leads against a defendant, but not disclosed, a defense attorney would not be able to confront or question that "witness."[127]

The Equal Protection Clause (EPC) of the Fourteenth Amendment requires states to treat similarly situated people equally under the law.[128] The EPC may offer limits to certain governmental usage of FRT technologies. In some circumstances, a state may have reasonable grounds for its unequal treatment of an individual. In *Heller v. Doe by Doe*, the Supreme Court stated that, "classifications neither involving fundamental rights nor proceeding along suspect lines do not run afoul of the Equal Protection Clause if there is a rational relationship between the disparity of treatment and a legitimate governmental purpose."[129] If an individual alleges discrimination, both state and federal courts will apply one of three levels of judicial scrutiny under the Equal Protection Clause to determine whether a governmental body's discrimination was permissible: rational basis review,[130] intermediate scrutiny,[131] or strict scrutiny.[132] The Court has stated:

> In considering whether state legislation violates the Equal Protection Clause of the Fourteenth Amendment, . . . we apply different levels of scrutiny to different types of classifications. At a minimum, a statutory classification must be rationally related to a legitimate governmental purpose . . . Classifications based on race or national origin, . . . and classifications affecting fundamental rights, . . . are given the most exacting scrutiny. Between these extremes of rational basis review and strict scrutiny lies a level of intermediate scrutiny, which generally has been applied to discriminatory classifications based on sex or illegitimacy.[133]

The Fourteenth Amendment requires prosecutors in a criminal action to disclose all evidence that is "favorable" and "material either to guilt or to punishment."[134] If a prosecutor were to rely on evidence from an FRT match, the Fourteenth Amendment may require them to disclose the use of

---

[126] *Davis v. Washington*, 547 U.S. 813, 822 (2006) ("Statements are nontestimonial when made in the course of police interrogation under circumstances objectively indicating that the primary purpose of the interrogation is to enable police assistance to meet an ongoing emergency. They are testimonial when the circumstances objectively indicate that there is no such ongoing emergency, and that the primary purpose of the interrogation is to establish or prove past events potentially relevant to later criminal prosecution.").
[127] *See, infra* note 221.
[128] U.S. Const. amend. XIV § 1 (""nor shall any State ... deny to any person within its jurisdiction the equal protection of the laws."); see, *Bolling v. Sharpe*, 347 U.S. 497 (1954) (noting the Court's interpretation of the 5th Amendment's Due Process Clause provides an equal protection requirement).
[129] 509 U.S. 312, 320 (1993).
[130] *Heller v. Doe by Doe* (applying rational basis review to determine discrimination on the basis of mental retardation).
[131] *Craig v. Boren*, 429 U.S. 190 (1976) (applying an "intermediate" level scrutiny to review discrimination on the basis of sex).
[132] *Korematsu v. United States*, 323 U.S. 214 (1944) (applying strict scrutiny to review discrimination on the basis of race).
[133] *Clark v. Jeter*, 486 U.S. 456, 461 (1988).
[134] *Brady v. Maryland,* 373 U.S. 83, 87 (1963); U.S. Const. amend XIV. The Supreme Court applied the due process clause of the Fifth Amendment to the Federal government to apply *Brady* to Federal prosecutions. *See Giglio v. United States,* 405 U.S. 150, 154 (1972), *U.S. v. Bagley*, 473 U.S. 667, 675 (1985).

FRT.[135] Although federal courts have not yet specifically ruled on this issue, the Superior Court of New Jersey held that the government was obligated to disclose detailed discovery information about the FRT tool used and the role it played in identifying the suspect.[136]

Federal Civil Rights Laws

The Civil Rights Act of 1964 prohibits discrimination based on race, color, religion, sex, and national origin in public accommodations, employment, and education, as well as by recipients of federal financial assistance. The Fair Housing Act of 1968 expanded the Civil Rights Act of 1964. It prohibits discrimination in the sale, rental, and financing of housing based on race, color, religion, national origin, sex, and (as amended) disability and family status. While federal civil rights laws do not explicitly contain provisions protecting against discriminatory usage of AI, several statutes afford some protection. For example, Title VII would prohibit federal agencies from using AI to screen applicants for employment in a discriminatory manner.[137]

Given that the focus of the Commission's current inquiry is the use of FRT by DOJ, DHS, and HUD, the most relevant provisions of federal statutory law are Title VI of the Civil Rights Act along with the Fair Housing Act.[138]

Section 601 of Title VI of the Civil Rights Act of 1964 states that "[n]o person in the United States shall, on the ground of race, color, or national origin, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving Federal financial assistance."[139] Title VI, however, extends only to "intentional discrimination."[140] In addition, the Fair Housing Act, which is enforced by DOJ and HUD, prohibits discrimination in housing on the basis of race, color, religion, sex, national origin, familial status, and disability.[141] "Title VI authorizes and directs federal departments and agencies that extend financial assistance to issue rules, regulations, or orders that effectuate the prohibition on discrimination on the basis of

---

[135] In *Brady v. Maryland,* the U.S. Supreme Court held that prosecutors must disclose evidence to the defense if it is exculpatory and material. *See Brady v. Maryland*, 373 U.S. 83 (1963).
[136] *State v. Arteaga,* 476 N.J. Super 36, *61 (App. Div. 2023).
[137] Jessica Kweon, *Artificial Intelligence ("AI"): Maryland's Double-Edged Sword in Employment Decisions*, 55 U. Balt. L.F. (forthcoming 2025); *See also*, EEOC, *Filing a Charge of Discrimination with the EEOC*, https://www.eeoc.gov/filing-charge-discrimination (advising that "if a person believes [they] have been discriminated against at work because of [their] race, color, religion, sex (including pregnancy, gender identity, and sexual orientation), national origin, age (40 or older), disability or genetic information, [they] can file a Charge of Discrimination" with the EEOC).
[138] 42 USC § 1983 provides a cause of action against state and local government employees for civil rights violations. A "Bivens action" is the federal analog which comes from *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971). Subject to certain exceptions, individuals deprived of rights provided by the Constitution by federal officers have a right under *Bivens* to recover damages in federal court. Given the narrow application of Bivens, further discussion of it is not necessary. *See* https://crsreports.congress.gov/product/pdf/LSB/LSB10500 for more information about *Bivens* claims. Likewise, a discussion of 42 USC § 1981 is largely unnecessary as it prohibits race discrimination in the making and enforcing of contracts and is therefore largely outside of the scope of FRT usage by HUD, DHS, and DOJ.
[139] Civil Rights Act of 1974, 42 U.S.C. § 2000d.
[140] *Alexander v. Sandoval*, 532 U.S. 275, 280 (2001).
[141] Fair Housing Act, 42 U.S.C. § 3601, et. seq.

race, color, or national origin."[142] Each of the departments this report covers have promulgated their own regulations under Title VI.

DOJ's Title VI regulations prohibit grant recipients from using funds in a manner that discriminates against certain protected classes. DOJ's recipients of federal funds may not, directly or through contractual or other arrangements, utilize criteria or methods of administration that have the effect of subjecting persons to discrimination because of their race, color, or national origin.[143] For example, a municipal police department receiving grant money from the DOJ may be in violation of the Title VI regulation if the department used DOJ grant money to purchase and use the FRT software in a manner that disproportionately misidentified people based on their race, leading to false arrests.

DOJ's Bureau of Justice Assistance (BJA) has provided grant awards in which funding was used to purchase FRT, in particular, through the Edward Byrne Memorial Justice Assistance Grant (JAG) Program. BJA informs potential grant recipients that in order for JAG funds to be used for FRT:

> [T]he recipient must have policies and procedures in place to ensure that the FRT will be used in an appropriate and responsible manner that promotes public safety; and protects privacy, civil rights, and civil liberties; and complies with all applicable provisions of the U.S. Constitution, including the fourth amendment's protection against unreasonable searches and seizures, the first amendment's freedom of association and speech, and other laws and regulations. Recipients utilizing funds for FRT must make such policies and procedures available to DOJ upon request.[144]

However, DOJ does not directly oversee other agencies. DOJ indicated that BJA has a current cooperative agreement to build digital trust with the National Policing Institute, through which BJA provides technical assistance, including reviews of agencies' policies related to FRT, to "ensure privacy, civil rights, and civil liberties are protected."[145]

DHS's Title VI implementing regulations, 6 C.F.R § 21 and 44 C.F.R.§ 7.5(b), prohibit intentional discrimination as well as discriminatory effects in Department-assisted programs and activities,[146] 6 C.F.R. § 21.5(b)(2) notes:

> A recipient, in determining the types of services, financial aid, or other benefits, or facilities which will be provided under any such program, or the class of person to whom, or the

---

[142] 42 U.S.C. §2000d-1; U.S. Dept. of Justice, *Title VI Legal Manual*, Section III, Department of Justice Role Under Title VI, Section III, p. 1, https://www.justice.gov/d9/books/attachments/2021/02/03/titlevi_legal_manual_rev._ed.pdf
[143] 28 C.F.R. § 42.104*; see* also U.S. Dept. of Justice, *Title VI Legal Manual*, Section VII, Proving Discrimination-Disparate Impact, p. 1, https://www.justice.gov/d9/books/attachments/2021/02/03/titlevi_legal_manual_rev._ed.pdf
[144] Bureau of Justice Assistance, "Bureau of Justice Assistance Edward Byrne Memorial Justice Assistance Grant (JAG) Program Frequently Asked Questions (FAQs)," https://bja.ojp.gov/doc/jag-faqs.pdf.
[145] U.S. Dep't of Justice, DOJ Responses to U.S. Commission on Civil Rights Interrogatories, Mar. 26, 2024.
The FBI has MOUs with 17 state agencies and two other federal agencies. With the exception of two of those 19 agencies, the personnel do not have direct login access, they transmit requests to the applicable agencies that run searches and return results.
U.S. Dep't of Justice, DOJ Responses to U.S. Commission on Civil Rights Interrogatories, Mar. 26, 2024.
[146] Department of Homeland Security, *Title VI Overview for DHS Recipients of Financial Assistance*, p. 1, https://www.dhs.gov/sites/default/files/publications/title-vi-overview-dhs-recipients.pdf

> situations in which, such services, financial aid, other benefits, or facilities will be provided under any such program, or the class of persons to be afforded an opportunity to participate in any such program; may not, directly or through contractual or other arrangements, utilize criteria or methods of administration which have the effect of subjecting persons to discrimination because of their race, color, or national origin or have the effect of defeating or substantially impairing accomplishment of the objectives of the program with respect to individuals of a particular race, color, or national origin.[147]

Thus, recipients[148] of the federal funds must ensure nondiscrimination both intentionally and based on disparate impacts in their activities and programs. However, as discussed above, the Supreme Court in *Sandoval* held that private parties [, i.e., beneficiaries] may not invoke Title VI regulations to obtain redress for disparate-impact discrimination because Title VI itself prohibits only intentional discrimination."[149]

HUD also promulgated its own rule effectuating Title VI of the Civil Rights Act of 1964. Regulation 24 C.F.R. § 1.4 notes that a recipient of federal funds, may not, directly or through contractual or other arrangements, utilize criteria or methods of administration have the effect of subjecting persons to discrimination because of their race, color, or national origin.[150]

Additionally, recipients of federal assistance from HUD may not "[r]estrict a person in any way in the enjoyment of any advantage or privilege enjoyed by others receiving any service, financial aid, or other benefit under the program."[151] For example, a public housing organization receiving grant money from HUD would be in violation of the department's regulation if it used surveillance cameras purchased with federal funds in a manner that restricted access to a public housing property for certain protected classes.[152]

Civil Rights Concerns

Civil rights concerns arising from widespread FRT usage are heightened by the technology's ease of deployment and ability to be used by inexperienced and inadequately trained operators. FRT's potential for surveillance and covert use, coupled with the widespread availability of personal information that can be associated with a facial image, magnify privacy concerns. Furthermore, the

---

[147] 6 C.F.R. § 21.5(b)(2)

[148] 6 C.F.R § 21.4(f) defines recipient as "…any State, territory, possession, the District of Columbia, or the Commonwealth of Puerto Rico, or any political subdivision thereof, or instrumentality thereof, any public or private agency, institution, or organization, or other entity, or any individual, in any State, territory, possession, the District of Columbia, or the Commonwealth of Puerto Rico, to whom Federal financial assistance is extended, directly or through another recipient, including any successor, assignee, or transferee thereof, but such term does not include any ultimate beneficiary."

[149] *See Jackson v. Birmingham Bd. of Educ*., 544 U.S. 167, 178 (2005) *citing* to *Alexander v. Sandoval*, 532 U.S. 275 (2001); *see* also DOJ Tile VI Legal Manual, Section IX, which is available here https://www.justice.gov/crt/fcs/T6Manual9.

[150] 24 C.F.R. §1.4 (b)(2)(i).

[151] 24 C.F.R. §1.4 (b)(1)(iv).

[152] *See, infra* notes 531, 543-545.

observed differences in false positive and false negative[153] match rates across phenotypes and demographic groups[154] raise equal protection concerns. The ability for surveillance to occur on a grand scale through the use of FRT prompts legal questions regarding the boundaries between permissible and non-permissible collection of data.[155] For example, the Fourth Circuit held in *Leaders of a Beautiful Struggle v. Baltimore Police Dep't* that using wide-angle aerial cameras to capture the movements of pedestrians and drivers across a whole city constitutes an unconstitutional general search.[156] The Commission received input from the American Civil Liberties Union (ACLU) indicating "[n]ot even a warrant could authorize such mass surveillance. Applying FRT to networks of surveillance cameras that already cover many U.S. cities would raise similar concerns."[157]

Accuracy

The National Institute of Standards and Technology (NIST) within the Department of Commerce has been working with public and private sectors in the area of biometrics since the 1960s.[158] Biometric technologies provide a way for users (e.g., private and/or public companies, law enforcement, federal agencies, and researchers) to establish or verify an individual's identity through the use of physical characteristics (e.g., face, fingerprint, and iris images). Participation in NIST testing is not mandatory; it is completely voluntary, free, and open to any organization worldwide.

Since 2000, NIST's Face Recognition Vendor Testing Program (FRVT) has assessed capabilities of facial recognition algorithms for one-to-one verification and one-to-many identification.[159] Patrick Grother, Supervisory Computer Scientist for the Information Technology Laboratory at NIST, provided testimony to the Commission, stating that "NIST biometric evaluations have measured the core algorithmic capability of biometric recognition technologies and reported the accuracy, throughput, reliability, and sensitivity of algorithms to data characteristics."[160] In other words, NIST tests developers' algorithms for accuracy (i.e., likelihood of the system returning false positives and/or false negatives), data processing volume, operational reliability, and sensitivity to noise (i.e., unnecessary other data or factors such as background images or distortion).

In 2023, the FRVT program was split into two parts: the Face Recognition Technology Evaluation (FRTE), which tests facial verification and identity algorithms, and the Face Analysis Technology Evaluation (FATE), which addresses facial analysis other than FRT, such as age estimation and face

---

[153] There are two error types that the software can make: false positives and false negatives. A false positive happens when the software inaccurately identifies a photo of two different individuals as the same person. Conversely, a false negative means the software failed to match two photos that, in fact, are of the same person. *See* Grother Statement, at 2.
[154] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.
[155] Nicol Turner Lee and Caitlin Chin-Rothmann, "Police surveillance and facial recognition: Why data privacy is imperative for communities of color," *Brookings,* Apr. 12, 2022, https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.
[156] *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330, 348 (4th Cir. 2021) (en banc).
[157] American Civil Liberties Union, Public Comment, Apr. 8, 2024 [on file].
[158] Grother Statement, at 1.
[159] Ibid., at 4.
[160] Ibid.

morphing.[161] Since testing is an ongoing process, algorithms are submitted on a continuous basis. Most commonly, algorithms are submitted to NIST by corporate research and development laboratories, as well as some universities.[162] Since 2017, NIST's FRTE evaluation has completed the evaluation of 1,633 prototypes from 376 developers.[163] NIST publishes on its website the performance reports and developer information from each of the algorithms it evaluates.

A 2019 NIST report found varying rates of accuracy among developers. The main result was that false positive differentials[164] (i.e., inaccurately attributing a photo of two different people as the same person) are much larger than false negative differentials (i.e., failing to match two images of one person as the same person) and exist broadly across many, but not all, tested algorithms.[165] Across different demographics, false positive differentials can vary by factors of 10 to beyond 100, depending on the algorithm. This means, depending on the algorithm and the demographics of the person, some people may be 10 to over 100 times more likely to have a false positive match result. False negatives tend to be more algorithm-specific and vary often by factors below 3.[166] The significance and implications of these differentials is discussed more below. It should be noted that false positive and false negative rates are determined by a cutoff threshold set for the algorithm by the user, and this threshold will often vary depending on the intended use for the FRT algorithm. For example, the threshold to unlock a smartphone is set high to prevent unauthorized access, and a user can enter a password if the FRT fails; yet airport security FRT thresholds would be set low for the sake of public safety, and a TSA agent can check the results against other information.[167]

Tests show that for identity verification (1:1 algorithms), the false positive match rates for certain demographic groups—even when using the best-performing facial recognition algorithms—are higher than for other groups. This is true even if both the probe and reference images are of high quality.[168] These demographic differentials found in verification algorithms are usually, but not always, present in identification (1:many algorithms).[169] This means that even with the highest-performing algorithms, tests have shown there are likely to be false positives for certain demographic

---

[161] Ibid.
[162] Ibid.
[163] Ibid., at 5.
[164] A differential means that an algorithm's ability to match two images of the same person varies from one demographic group to another. For some demographics, the false positive rate could be a factor of 10, but for others it could be higher than 100 (e.g., differences in false positives between White men and African women). *See*, National Institute of Standards and Technology, "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.
[165] National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,* Dec. 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[166] National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,* Dec. 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
It is important to consider, additionally, that NIST fixes the false negative rate to determine the false positive rate: they are a tradeoff. If the threshold is moved it could increase the false negative rate and reduce the false positive rate at the same time. DOJ Affected Agency Review, Jun. 21, 2024.
[167] Example provided by DOJ Affected Agency Review, Jun. 21, 2024.
[168] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.
[169] Ibid.

groups, specifically Black people, people of East Asian descent, women, and older adults than over the entire population. Additionally, these inaccuracies are still apparent even after controlling for image quality. The racial differentials are largely due to these algorithms being designed in Western countries and trained mostly on White faces. A discussion on the civil rights implications of differentials is discussed below.[170]

Scale is another important consideration when examining various algorithms for accuracy. For instance, if a developer has an accuracy rate of 99 percent, the 1 percent misidentification rate may be substantial depending on the number of images (i.e., people) it is trying to differentiate between. Bertram Lee, a technology policy expert, testified that while some developers claim their algorithms are 99.8 or 99.9 percent accurate, if the system is running a 1:many operation, that could mean that hundreds or even thousands of people may be misidentified.[171] In a real-world scenario, this misidentification could mean, if the technology is overly relied upon, that an innocent person is detained or even arrested due to the algorithm mistaking them for someone else.[172]

Proponents of FRT point to the fact that while misidentification (either false positives or false negatives) may occur, the algorithms are still superior to human identification and eyewitness accounts. Longstanding research shows that eyewitness identifications are often unreliable, especially when the alleged perpetrator and witness are of different races.[173] Katie Kinsey, Chief of Staff at New York University Law School's Policing Project, argues that the notion of FRT being able to eliminate eyewitness misidentification is a "false premise," because "facial recognition is a process that involves human reviewers at multiple points in the process."[174] Kinsey explained that the process often involves one officer reviewing the algorithm's results to confirm them, another officer reviewing that confirmation, and then potentially having an eyewitness confirm that finding. Thus, she argues, the same problems inherent in eyewitness identification are potentially compounded.[175] Also, the issue of misidentification can be amplified due to FRT being proficient in providing look-alikes, which makes the task for the human reviewer more difficult, as humans are not good at distinguishing unfamiliar faces.[176]

Additionally, FRT human reviewers are not immune from "automation bias," or the propensity for humans to inordinately favor suggestions from automated decision-making systems and to ignore or fail to seek out contradictory information made without automation.[177] That said, when performing

---

[170] *See infra* notes 184-214.
[171] Bertram Lee, Technology Policy Expert, testimony, *Facial Recognition Technology Briefing,* p. 66-67.
[172] Alyxaundria Sanford, "Artificial Intelligence Is Putting Innocent People at Risk of Being Incarcerated," *Innocence Project,* Feb. 14, 2024, https://innocenceproject.org/artificial-intelligence-is-putting-innocent-people-at-risk-of-being-incarcerated/.
[173] Christian A. Meissner and John C. Brigham, "Thirty years of investigating the own-race bias in memory for faces: A meta-analytic review," *Psychology, Public Policy, and Law,* 2001, vol. 7, no. 1, 3–35. https://doi.org/10.1037/1076-8971.7.1.3.
[174] Kinsey Testimony, p. 82.
[175] Ibid.
[176] Ibid., p. 83.
[177] Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," Mar. 28, 2024,

with high accuracy, the technology can be more accurate than the human eye, and thus, less subject to the faulty memories and inherent biases often seen using eyewitness identifications.[178] Clearview AI CEO and Founder Hoan Ton-That stated in his written testimony that "[b]y reducing the need to rely on human eyewitnesses, we reduce reliance on one of the most inaccurate and racially biased identification methodologies in criminal justice."[179]

Despite the small known number[180] of erroneous identifications nationwide, Assistant Chief Armando Aguilar testified to the Commission that the Miami Police Department has never used FRT to identify a suspect who was later exonerated using other means.[181] While this is the experience of only one police department, it exemplifies how continued improvement of FRT algorithms and user training, can reduce the number of misidentifications that lead to false arrests and possibly result in these errors becoming statistically nonexistent.

Studies conducted by DHS S&T have demonstrated improved accuracy of FRT. For example, a controlled scenario test showed promising results for FRT to accurately identify individuals wearing protective face masks approximately 96 percent of the time with the best performing system (with a median system performance demonstrating a 77 percent identification rate).[182] Without masks, median system performance demonstrated a 93 percent identification rate, with the best-performing system correctly identifying individuals about 100 percent of the time.[183]

Potential Bias

One of the biggest concerns regarding the use of FRT is whether accuracy issues lead to bias, especially toward people of color. This critique of technology predates the development of FRT. Technology policy expert Bertram Lee noted in his written testimony:

> Camera technologies are historically racist, as there has been a long struggle for darker skinned people to have their images accurately captured on camera. The ability to photograph a wide variety of darker skin tones was only created because of the need to capture chocolate accurately for advertisement purposes.[184]

---

https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.

[178] Ton-That Statement, at 3.

[179] Ton-That Statement, at 3.

[180] As of February 2024, there have been seven confirmed cases of misidentification due to the use of facial recognition technology. *See* Alyxaundria Sanford, "Artificial Intelligence Is Putting Innocent People at Risk of Being Incarcerated," *Innocence Project,* Feb.14, 2024, https://innocenceproject.org/artificial-intelligence-is-putting-innocent-people-at-risk-of-being-incarcerated/.

[181] Armando Aguilar, Assistant Chief, Miami Police Department, Response to Follow-Up Questions, p. 1 [on file].

[182] DHS Science and Technology Directorate, "News Release: Airport Screening While Wearing Masks? Facial Recognition Tech Shows up to 96% Accuracy in Recent Test," Jan. 4, 2021, https://www.dhs.gov/science-and-technology/news/2021/01/04/news-release-airport-screening-while-wearing-masks-test.

[183] Ibid.

[184] Lee Statement, at 2; *see also* Sarah Lewis, "The Racial Bias Built Into Photography," *The New York Times,* Apr. 25, 2019, https://www.nytimes.com/2019/04/25/lens/sarah-lewis-racial-bias-photography.html.

Nicol Turner Lee, Senior Fellow for Governance Studies and Director of the Center for Technology Innovation at the Brookings Institute and contributor to the National Academy of Scientist report, explained that in the 1950s, large camera manufacturers like Kodak began using "Shirley Cards," an image of a White Kodak employee to calibrate film production. This led to Black people being visually obscured in photographs.[185] It was not until the mid-1990s that Kodak produced a multiracial Shirley Card to address the issue. Today, photography still struggles to "capture Black skin accurately."[186]

Turner Lee wrote:

> Although the digital photograph technology now used in surveillance cameras worldwide works differently, similar problems persist, and photogenic methods still perform poorly for people with darker-skinned complexions, and equipment failures, like low quality cameras or poorly lit settings, deliver false results for Black people – only this time in more consequential settings.[187]

In December 2019, NIST released Interagency Report 8280, which quantified the effect of age, race, and sex on facial recognition performance.[188] The report analyzed 1:1 verification and 1:many search algorithms separately and found that demographic differences in false positive rates are often much larger than those for false negatives. [189] False positive rates were highest in West and East African and East Asian people, and lowest in Eastern European individuals.[190] The effect was generally large, with a factor of 100 more false positives between countries. However, for a number of algorithms developed in China, this effect was reversed, with low false positive rates for East Asian faces. [191] With domestic law enforcement images, the highest false positives were in American Indians, with elevated rates in Black and Asian populations.[192] While the NIST studies have not explored the relationship between cause and effect, the AI literature documents many instances where imbalanced training data cause underperformance with underrepresented groups.[193]

Regarding false negatives, NIST tests show that they are higher among images of Asian and American Indian individuals, with error rates above those in Black and White faces in U.S. domestic arrest photos. Border crossing images, which are often lower quality, yielded higher false negatives among people born in Africa and the Caribbean, with differing results relating to image quality.[194]

---

[185] Nicol Turner Lee, Senior Fellow, Governance Studies and Director of the Center for Technology Innovation, Brookings Institute, Written Statement for the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, at 4 (hereinafter Turner Lee Statement).
[186] Amanda Levendowski, *Resisting Face Surveillance with Copyright Law,* 104 N.C. L. Rev. 1015 (2022) (Introduction, I. A), https://scholarship.law.georgetown.edu/facpub/2457/.
[187] Turner Lee Statement at 4-5.
[188] National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,* Dec. 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[189] Grother Statement, at 5-6.
[190] National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,* Dec. 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[191] Ibid.
[192] Ibid.
[193] Grother Statement, at 6.
[194] National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,* Dec. 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

The poor quality of images taken at the border is particularly important for the Department of Homeland Security to take into consideration when utilizing FRT, and this is discussed in Chapter 2.

NIST testing is ongoing, and the analysis criteria applied to algorithms in the 2019 report are now applied to all algorithms submitted to the FRTE benchmark.[195] Patrick Grother explained that NIST has documented increased accuracy over the last decade, and these advancements are continuing. However, "[w]hile the industry gains are broad, there remains a wide range of capabilities, with some developers providing much more accurate algorithms than others."[196] In 2022, NIST published Interagency Report 8429 to establish summary measures for stating the overall magnitude of demographic effects.[197] The report explains:

> Since 2019, it has become apparent that false negative inequities are substantially due to poor photography of certain groups including under-exposure of dark-skinned individuals, and that this can be addressed by using algorithms more tolerant of poor image quality or, better, by correcting the capture process with superior cameras, imaging environments and human-factors. At the same time, it is also clear that the much larger false positive variations, which occur even in high-quality photographs, must be mitigated by algorithm developers.[198]

NIST emphasizes the importance of false positive differentials, particularly, because the algorithm's developer is responsible for their remediation and develop more accurate algorithms, while false negatives may be remediated by better photography.[199] NIST plans to publish a demographics report for recently submitted 1:many search algorithms later in 2024.[200]

As Grother testified:

> For both facial recognition and facial analysis algorithms, a general takeaway from these studies is that algorithms vary significantly, that is, some produce significantly fewer errors than others. Consequently, users, policy makers, and the public should not think of facial recognition and analysis as either always accurate or always error prone.[201]

The risk of error, then, could be reduced somewhat if agencies only used algorithms that exhibited high overall accuracy rates and eliminated tested-for accuracy biases.[202] However, the U.S. currently "lacks a regulatory and financial incentive structure, as well as the necessary levels of transparency and internal expertise, to make this a reality."[203] Additionally, the algorithm is just one element of

---

[195] Grother Statement, at 4.
[196] Ibid.
[197] National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 8: Summarizing Demographic Differentials,* Jul. 2022, https://pages.nist.gov/frvt/reports/demographics/nistir_8429.pdf.
[198] Ibid.
[199] Ibid.
[200] Grother Statement, at 6.
[201] Ibid., at 7.
[202] Georgetown Law Center on Privacy & Technology, *A Forensic Without The Science: Face Recognition in U.S. Criminal Investigations,* Dec. 6, 2022, https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/.
[203] Ibid.

the search. Any conclusion about the reliability of facial recognition based on algorithm performance alone would fail to take into account the majority of stages in the search process.[204] For instance, in almost all organizations an FRT match is required to be verified by a human reviewer, thus introducing both an additional fail-safe and an additional step for error to occur.[205] Moreover, an algorithm tested using the NIST database may not perform as well in real-world applications,[206] such as with images captured on CCTV that are grainier and less defined.[207] To gain a better understanding of how FRT is tested, as a component of this project, the Commission visited a DHS contracted test lab in Maryland on April 18, 2024. A full description of the site visit is discussed in Chapter 2.

Concern over FRT use center on that the reliability and accuracy of the algorithm cannot be fixed if the database itself is not diversified. Unless the databases have access to diverse data, these programs will continue to perform poorly when attempting to recognize Black American or Asian American features.[208] One of the most important factors in reducing bias appears to be the selection of data used to train algorithmic models. If algorithms are trained on data sets that contain very few examples of a particular demographic group, the resulting model will be worse at accurately recognizing members of that group in real-world deployments.[209] An FRT system can extrapolate information from under or unrepresented groups, albeit with increased error.[210]

Heather Roff, Associate Fellow in the University of Cambridge's Leverhulme Centre for the Future of Intelligence, and Senior Research Scientist at the Center for Naval Analysis, testified:

> For FRT, we may say that systems should be trained on a large enough sample size of the given demographics of any given country. If the country is multi-racial, multi-cultural, etc., then that data should reflect this, so that the AI model has "seen" enough images of individuals representing these groups/classes to be able to make identification.[211]

The selection of the datasets and data source (i.e., photos) is also a significant concern to ensure that the technology responds equitably across all demographic groups. Many FRT databases, especially those utilized by law enforcement, are constructed through arrest photos and driver's license photos. Congressman Ted Lieu, in his written statement to the Commission, raises the concern that, due to longstanding racial biases in the criminal justice system, building a system from arrest photos, where people of color are overrepresented, could also lead to racial biases in FRT.[212]

---

[204] Ibid.
[205] *See, supra* notes 173-176.
[206] FRT testing within a laboratory environment may perform differently than in the field since variables can be altered at will, closely monitored, and controlled. *See* discussion of the Commission's site visit with the Maryland Test Facility, notes 460-505.
[207] *See, infra* note 247.
[208] Darrell M. West and John R. Allen, "How artificial intelligence is transforming the world," *Brookings,* Apr. 24, 2018, https://www.brookings.edu/articles/how-artificial-intelligence-is-transforming-the-world/.
[209] William Crumpler and James A. Lewis, "How Does Facial Recognition Work?" *Center for Strategic and International Studies,* Jun. 10, 2021, https://www.csis.org/analysis/how-does-facial-recognition-work.
[210] DOJ Affected Agency Review, Jun. 21, 2024.
[211] Heather Roff, Associate Fellow, Leverhulme Centre for the Future of Intelligence, University of Cambridge & Senior Research Scientists, Center for Naval Analysis, Responses to Follow-Up Questions, p. 1 [on file].
[212] Representative Ted Lieu, Member of the House Judiciary Committee, Written Statement for the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, at 3 (hereinafter Lieu Statement).

Error rates are reported at the aggregate level, which may also hide some of the harms behind algorithms. Joy Buolamwini of the Algorithmic Justice League and the author of Unmasking AI wrote in her testimony to the Commission that as of her writing, according to the top-listed algorithm on the NIST leaderboard, the "ratio of the best performance to the worst performance shows that West African women (65 years of age and older) were over 3,000 times more likely to have a false positive match than Eastern European men (20 - 35 years of age) in the worst case."[213] Those women were 15 times more likely to have a false positive match than the average case against all demographics.[214]

Law Enforcement Use of FRT

The use of FRT by law enforcement is one of the most prevalent examples of the technology's application in real-world applications. Understanding how local and federal law enforcement utilize FRT can offer some valuable insights about the potential benefits and risks of the technology and how it is deployed throughout various criminal justice system elements.

While FRT has been used to assist in criminal investigations, the use raises privacy and accuracy concerns, especially when it comes to known differentials applied to racial minorities. Facial recognition software has assisted police in identifying suspects, such as the captured suspect of the mass shooting at the *Capital Gazette* newsroom in 2018.[215] However, there have also been several instances of wrongful arrests following the use of FRT.[216]

An independent investigation found that in a 2021 GAO report surveying 42 federal law enforcement agencies' use of facial recognition, five agencies claimed they did not use Clearview AI between April 2018 and March 2020, but internal Clearview AI data indicated otherwise.[217] Os Keyes, a researcher on the politics of AI systems, said this discrepancy "speaks to the fact that the GAO analysis … is ultimately playing catchup, and in a domain where … people are not documenting the technologies they use, the regulations they put around them, or the processes for accessing them."[218]

---

[213] Buolamwini Statement, at 9.
[214] Ibid.
[215] Dyllan Furness, "Police used facial recognition software to identify the Capital Gazette shooter," *Digital Trends,* Jun. 29, 2018, https://www.digitaltrends.com/cool-tech/capital-gazzette-shooter-facial-recognition/.
[216] *See* Elaisha Stokes, "Wrongful arrest exposes racial bias in facial recognition technology," *CBS News,* Nov. 19, 2020, https://www.cbsnews.com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime/; Kashmir Hill, "Eight Months Pregnant and Arrested After False Facial Recognition Match," *The New York Times,* Aug. 6, 2023, https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html; Johana Bhuiyan, "Facial recognition used after Sunglass Hut robbery led to man's wrongful jailing, says suit," *The Guardian,* Jan. 22, 2024, https://www.theguardian.com/technology/2024/jan/22/sunglass-hut-facial-recognition-wrongful-arrest-lawsuit; Drew Harwell, "Man sues Macy's, saying false facial recognition match led to jail assault," *The Washington Post,* Jan. 22, 2024, https://www.washingtonpost.com/technology/2024/01/22/facial-recognition-wrongful-identification-assault/; Christina Swarns, "When Artificial Intelligence Gets It Wrong," *Innocence Project,* Sept. 19, 2023, https://innocenceproject.org/when-artificial-intelligence-gets-it-wrong/.
[217] Caroline Haskins and Ryan Mac, "A Government Watchdog May Have Missed Clearview AI Use By Five Federal Agencies In A New Report," *Buzzfeed News,* Jun. 30, 2021, https://www.buzzfeednews.com/article/carolinehaskins1/gao-facial-recognition-report-clearview-federal-agencies.
[218] Ibid.

As early as 2016, the Georgetown Law Center on Privacy & Technology reported that law enforcement facial recognition networks included over 117 million American adults.[219] The report explained:

> Historically, FBI fingerprint and DNA databases have been primarily or exclusively made up of information from *criminal* arrests or investigations. By running face recognition searches against 16 states' driver's license photo databases, the FBI has built a biometric network that primarily includes *law-abiding Americans*.[220]

Clare Garvie, Fourth Amendment Center's training and resource counsel at the National Association of Criminal Defense Lawyers (NACDL), testified that while FRT has been used in hundreds of thousands of criminal cases, its use is rarely disclosed to the defense.[221] Since the majority of cases are resolved through plea bargaining, this can further decrease transparency around law enforcement's use of FRT. Garvie explains that when a case pleads out, the court does not examine the state's obligation under *Brady*[222] to disclose how a search was run, and "never rules on important legal questions surrounding the use of facial recognition in policing."[223]

At the Commission's briefing, Chief Armando Aguilar of the Miami Police Department explained that FRT is only one part of the process that officers in his department use when searching for an alleged perpetrator. He testified that after generating a "hit":

> [T]hat detective has to go out and do their due diligence, for example, putting a photograph of that suspect into a photographic lineup… [W]e are not running out and making an arrest just because an algorithm tells us to do so… [and] I think that it [] speaks to the due diligence that is happening on the human side of that investigation and saying, great, we have this match. Let's gather as much evidence from other sources, [such as], physical testimony or circumstantial evidence as we can to either make this case or not.[224]

Similarly, Founder and CEO of Clearview AI Hoan Ton-That states that he is "a true believer that there should be a human judgment at the end of the day. I don't believe in automated decision-making at all… So, I think for investigators, the more information that confirms who someone is, [or] that disconfirms who someone is, can be very valuable."[225] Brian Finch, law partner at Pillsbury Law, agrees and testified that "facial recognition should be viewed as a lead generator. And that

---

[219] Georgetown Law Center on Privacy & Technology, *The Perpetual Line-Up: Unregulated Police Face Recognition in America,* Oct. 18, 2016, https://www.perpetuallineup.org/.
[220] Ibid (emphasis in original).
[221] Garvie Testimony, p. 207.
[222] *Brady v. Maryland*, 373 U.S. 83 (1963).
[223] Garvie Testimony, pp. 210-211.
[224] Armando Aguilar, Assistant Chief, Miami Police Department, Testimony before the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, pp. 76-78 (hereinafter Aguilar Testimony).
[225] Hoan Ton-That, Founder and CEO, Clearview AI, testimony, *Facial Recognition Technology Briefing,* pp. 58-59.

should be its main purpose, to be followed by human intervention, human review, and continuous auditing."[226]

In January 2020, Clearview AI indicated that more than 600 law enforcement agencies had been using its technology in the past year,[227] and in a 2021 interview with *Wired*, Ton-That indicated the company has 3,100 law enforcement and government customers.[228] In his written testimony to the Commission, Ton-That stated that each law enforcement agency using Clearview must assign an administrator to conduct audits to ensure that every search is for a legitimate purpose.[229] He continued:

> Every law enforcement officer that uses Clearview AI must identify each search and document its purpose by assigning a crime type and case number for each search, ensuring that all searches are tied to a legitimate investigation. Each law enforcement agency must also assign an administrator that conducts audits to ensure that every search is for a legitimate purpose.[230]

The Georgetown Law Center on Privacy & Technology report explained that the "human backstop to accuracy"—the reliance on having a police officer decide whether a candidate photo is a match—is non-standardized and overstated.[231] While having a human review the results may be a useful safeguard against false matches, a 2015 study found that without specialized training, human reviewers make the wrong decisions about matches about half the time.[232] Heather Roff echoed this concern, testifying:

> Just because there's a human there doesn't mean that the human's going to be responsible. You could be creating a human patsy and saying well that guy said it was yes and so therefore it's okay. That's not something we want to do; we want to have meaningful engagement and appropriate human judgment when looking at that system. So, I would say we can utilize these systems, but we must ensure that the way in which they're being double checked is in this kind of dual phenomenology and not over-relying on automated tools.[233]

---

[226] Brian Finch, Partner, Pillsbury Law, Testimony before the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, p. 226 (hereinafter Finch Testimony).
[227] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times,* Jan. 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[228] Will Knight, "Clearview AI Has New Tools to Identify You in Photos," *Wired,* Oct. 4, 2021, https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos/.
[229] Ton-That Statement, at 2.
[230] Ibid.
[231] Georgetown Law Center on Privacy & Technology, *The Perpetual Line-Up: Unregulated Police Face Recognition in America,* Oct. 18, 2016, https://www.perpetuallineup.org/.
[232] White, D., Dunn, J. D., Schmid, A. C., & Kemp, R. I. (2015). "Error Rates in Users of Automatic Face Recognition Software," *PLoS ONE 10*(10): e0139827. https://doi.org/10.1371/journal.pone.0139827.
[233] Heather Roff, Associate Fellow, Leverhulme Centre for the Future of Intelligence, University of Cambridge & Senior Research Scientists, Center for Naval Analysis, Testimony before the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, p. 230 (hereinafter Roff Testimony).

In a 2022 Pew Research Center study assessing Americans' opinions regarding widespread use of FRT by law enforcement, researchers found that most of the American public believes widespread use of FRT would likely help find missing persons and solve crimes, but a majority also think it is likely that police would use this technology to track everyone's location and surveil Black and Latino communities more than others.[234] A substantial share (64 percent) said the use of the technology by police would be more acceptable if police officers were trained in how facial recognition systems can make errors in identifying people before they use it.[235] When asked about who should play a role in setting standards for police use of facial recognition technology, roughly half of Americans say the police departments that use this technology (51 percent) and federal government agencies (49 percent) should play a major role. Smaller shares say that companies that develop facial recognition technology (41 percent) and ordinary people (40 percent) should play a major role in setting standards for how the technology is used by police.[236]

Over the years, some cities and states have enacted legislation banning or restricting law enforcement's use of FRT, only to reverse course over time. For instance, New Orleans passed an ordinance in 2020 banning police from using FRT, but in July 2022, the city determined that officers could request permission from a superior to use the software for violent crime investigations.[237] Virginia outlawed local and campus police from using facial recognition in 2021, and then enacted a law in 2022 allowing it in some situations.[238] California's legislature passed a three-year law in 2020 that prohibited all law enforcement from using facial recognition.[239] The ban has since expired, and the state has been mired in divisions over various State Assembly bills aimed at regulating law enforcement's use of FRT.[240]

Despite its increasing use, there is no publicly available data regarding the accuracy of law enforcement use of FRT in its actual practice. In written testimony to the Commission, Clare Garvie wrote:

> We have no ground truth data for how often the police facial recognition searches get it right—or wrong. This is particularly true given the rates at which cases plead out and the known risk that people—particularly indigent defendants—plead guilty to crimes they didn't

---

[234] Lee Rainie, Cary Funk, Monica Anderson, and Alec Tyson, "2. Public more likely to see facial recognition use by police as good, rather than bad for society," *Pew Research Center,* Mar. 17, 2022, https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society/.
[235] Ibid.
[236] Ibid.
[237] Rachel Metz, "First, they banned facial recognition. Now they're not so sure," *CNN,* Aug. 5, 2022, https://www.cnn.com/2022/08/05/tech/facial-recognition-bans-reversed/index.html.
[238] Ibid.
[239] Ibid.
[240] *See* Lindsay Holden, "Divisions Grow Over Use of Facial Recognition in California," *GovTech,* Apr. 18, 2023, https://www.govtech.com/policy/divisions-grow-over-use-of-facial-recognition-in-california; CBS News, "Bill proposed to regulate facial recognition technology in policing," Mar. 8, 2023, https://www.cbsnews.com/sanfrancisco/news/bill-proposed-to-regulate-facial-recognition-technology-in-policing/; Titus Wu, "California at Crossroads Over Policing and Facial Recognition," *Bloomberg Law,* Mar. 29, 2023, https://news.bloomberglaw.com/privacy-and-data-security/california-at-crossroads-over-policing-and-facial-recognition.

> commit to avoid a "trial penalty," [or] the risk of facing exponentially higher sentences should they invoke their right to trial and lose. Perhaps more importantly, however, this is not a laboratory setting, where margins of error may be acceptable; this is our criminal legal system. These are real people whose lives are irreparably harmed by a wrongful arrest.[241]

Additionally, the extent to which departments are using FRT, including which programs or algorithms they are using, is not always publicly available. Katie Kinsey, Chief of Staff at NYU Law's Policing Project, explained in her written statement that:

> Fundamental questions – such as how often agencies run searches, for what types of crimes, on what demographics, and to what result – remain unanswered. What little public information does exist about federal law enforcement use stems largely – sometimes exclusively – from investigative reporting or is scattered across federal auditor reports – and not, as it should, from agencies' affirmative commitments to transparency, publicly available policies, or democratically-enacted legislation.[242]

However, the extent to which FRT has helped law enforcement agencies should not go unmentioned. Armando Aguilar, Assistant Chief of Miami Police Department, testified that his department has successfully leveraged FRT and other AI in the past few years, to great effect and while employing a carefully constructed facial recognition policy (see Chapter 3).[243] The Commission also received a public comment from the Security Industry Association, emphasizing:

> As the importance of limiting human bias in police work as well as limiting unnecessary interactions with citizens becomes increasingly clear, biometric technology makes the process of generating and investigating leads much faster and more accurate than relying only on human analysis alone.[244]

External Validity

While NIST conducts testing on various programs submitting their 1:1 and 1:many FRT algorithms, it is important to understand what the current research on accuracy and bias does not tell us. External validity is the extent to which findings are relevant to settings beyond the initial study, essentially, the generalizability of the findings.[245]

The 2019 NIST Demographic Effects report does not indicate how all FRT in use is performing. Rather, the report was an analysis of "189 mostly commercial algorithms from 99 developers."[246]

---

[241] Garvie Statement, p. 5.
[242] Kinsey Statement, p. 4.
[243] Armando Aguilar, Assistant Chief, Miami Police Department, Written Statement for the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, at 2-3 (hereinafter Aguilar Statement).
[244] Security Industry Association, Public Comment for the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, Apr. 8, 2024 [on file].
[245] Vogt, W. P. (Ed.) (2005). Dictionary of statistics & methodology. (Vols. 1-0). SAGE Publications, Inc., https://doi.org/10.4135/9781412983907.
[246] National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,* Dec. 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

As stated previously, NIST testing is voluntary, and developers decide if they want to submit their algorithms for testing. Therefore, NIST testing reports provide a snapshot of a group of FRT programs at a given time and thus cannot say those programs are representative of the accuracy of all FRT throughout the country. Nor do the programs reflect the real-world accuracy of a specific program being used by a specific agency. For example, there is not always publicly available testing of FRT systems used by law enforcement using the types of images they may use for searches, such as low-resolution or grainy images from sources such as security and CCTV cameras.[247]

Thus, when a prominent law enforcement FRT vendor such as Clearview AI states that in the NIST testing, its algorithm found the correct face out of a lineup of 12 million photos at an accuracy rate of 99.85 percent,[248] this result is only applicable in laboratory settings and does not necessarily reflect the algorithm's accuracy rate in how it may be operationally used by law enforcement. In its recently issued guidance on the federal government's use of AI, the Office of Management and Budget (OMB) requires that, no later than December 1, 2024, before using covered new or existing safety-impacting or rights-impacting AI, federal agencies:

> must conduct adequate testing to ensure the AI, as well as components that rely on it, will work in its intended real-world context. Such testing should follow domain-specific best practices, when available, and should take into account both the specific technology used and feedback from human operators, reviewers, employees, and customers that use the service who impact the system's outcomes. Testing conditions should mirror as closely as possible the conditions in which the AI will be deployed.[249]

Katie Kinsey of the Policing Project explained in her written statement:

> To understand why NIST testing isn't sufficient, consider the testing required for another human-machine system: a Formula 1 racecar. NIST's algorithm testing would be the equivalent of just testing a Formula 1 car's engine in isolation. If you own a Formula 1 racecar, you might start with engine testing, but you don't stop there. You're also going to test how the engine performs in the actual car, with a driver, on a racetrack. In other words, you're going to test your racecar in real-world conditions.[250]

The OMB guidance requires agencies to conduct adequate testing to ensure AI will work as intended in an FRT system used for certain functions in the law enforcement context. As Heather Roff wrote in her statement to the Commission, FRT is not used just for the sake of running facial recognition, it is used for a particular purpose.[251] This means that, mathematically, when a user integrates an

---

[247] Kinsey Statement, at 3.
[248] Ton-That Statement, at 1.
[249] Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," Mar. 28, 2024, pp. 18-19, https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.
[250] Kinsey Statement, at 4.
[251] Heather Roff, Associate Fellow, Leverhulme Centre for the Future of Intelligence, University of Cambridge and Senior Research Scientist, Center for Naval Analysis, Written Statement for the Civil Rights Implications of the

automated system into a larger system or a "system of systems," with each component having its own error rate, this can cause real world problems and lead to possible civil rights violations.[252] Without knowing those error rates on the front end and where FRT is used in the system, there may be higher probabilities of error and more difficulty identifying where those errors occurred.[253] Roff explained at the Commission briefing:

> So, if my face comes up and it says . . . "you committed sexual assault, it was you," and you go, "it wasn't me, I wasn't there." But your face says that you were there, there's not a lot else, if all of the other information that I'm using to say it was you, it was your face. It's actually all the other automated information that I'm getting about your network connections, about whether or not you were in the location. Was your car there? Was there an automatic plate reader? All of that information that's also feeding into [it], but your face came up too. So, it's not just facial recognition by itself, it's all of the other systems and their compounded error rates together that give you that false positive.[254]

Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, at 3 (hereinafter Roff Statement).
[252] Roff Statement, at 3.
[253] Ibid.
[254] Roff Testimony, pp. 228-29.

[This page is left intentionally blank]

CHAPTER 2: The Use of Facial Recognition Technology by the Federal Government

As discussed in the previous chapter, the use of FRT has become increasingly common across the federal government. In August 2021, the GAO found that FRT was being used throughout the federal government, with 18 of 24 surveyed agencies reporting FRT use for one or more purposes.[255] In another study of 42 agencies that employ law enforcement officers, 14 of those agencies utilized FRT. Of those, 13 "did not track employee use of non-federal (e.g., state and commercial) FRT systems."[256] GAO found that these agencies were not aware that their employees were using non-federal (e.g. state or commercial) FRT and yet had conducted more than 1,000 facial recognition searches. This has serious implications, including impacting federal agencies' ability to ensure compliance with privacy laws.[257]

As the usage of FRT increases among federal agencies, civil rights concerns also grow. While a full discussion of the federal utilization of the technology is outside the purview of this report, the Commission focuses on three departments: the Departments of Justice, Homeland Security, and Housing and Urban Development to explore how FRT is being used, whether any training is in place, civil rights concerns regarding FRT usage, and what the government is doing to address these concerns.

U.S. Department of Justice (DOJ)

Under the leadership of the Attorney General of the United States, the Justice Department has a broad mandate to "uphold the rule of law; to keep our country safe from all threats, foreign and domestic; and to protect civil rights."[258] DOJ is composed of many different organizations and agencies, but for this report, the Commission focuses on FRT usage by the Federal Bureau of Investigation (FBI) and the United States Marshals Service (USMS). In the Department's written statement to the Commission, it explained that the FBI, USMS, and the Child Exploitation and Obscenity Section of the Criminal Division operate FRT systems.[259] The other law enforcement agencies such as the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Drug Enforcement Administration (DEA), and the Bureau of Prisons (BOP) do not currently operate FRT systems.[260]

FRT Utilization

FBI

[255] Candice N. Wright, "Facial Recognition Technology: Federal Agencies' Use and related Privacy Protections," U.S. Government Accountability Office, Testimony Before the Subcommittee on Investigations and Oversight, Committee on Science, Space, and Technology, Jun. 29, 2022, https://www.gao.gov/assets/gao-22-106100.pdf
[256] Ibid.
[257] Ibid.
[258] *See generally*, U.S. Dep't of Justice, FYs 2022-2026 Strategic Plan, https://www.justice.gov/file/1225821/dl?inline.
[259] DOJ Statement, at 5.
[260] Ibid.

According to the DOJ, the FBI uses FRT to "fulfill its mission to protect the American people in a manner consistent with the constitutional, statutory, regulatory, and policy frameworks that guide all FBI activities, in addition to the Department's interim FRT Policy and component policies specific to the procurement, tracking, evaluation, and use of FRT."[261] The FBI uses its own proprietary programs, which can be supported by proprietary or commercially available algorithms, as well as commercial or third-party services that are FRT systems or that contain an element of FRT.[262]

The FBI's Criminal Justice Information Services (CJIS) Division operates two programs that support the FBI's use of FRT: (1) the Next Generation Identification–Interstate Photo System (NGI-IPS), largely supporting federal, state, and local law enforcement; and (2) the Facial Analysis, Comparison, and Evaluation (FACE) Operations Services, supporting FBI investigations.[263]

NGI-IPS

The NGI-IPS contains all face images (e.g., arrest photos) received with ten print fingerprint transactions voluntarily submitted by authorized federal, state, local, tribal, territorial, and select foreign and international agencies. According to the FBI, the NGI-IPS permits broader acceptance and use of photos by allowing: (1) more photo sets per criminal subject in FBI records, (2) the bulk submission of photos maintained at state repositories, and (3) the submission of photos that are not of faces (e.g., scars, marks, and tattoos).[264] The NGI-IPS provides an investigative facial recognition (FR) search capability that allows authorized law enforcement agencies to search probe photos against the arrest photos housed in the NGI IPS to assist with ongoing investigations. To search the NGI IPS, an authorized law enforcement agency must adhere to the *NGI IPS Policy and Reference Guide* which denotes the procedural, legal, policy, training, and technical requirements that must be met before requesting an investigative FR search of the NGI IPS. Authorized law enforcement agencies submit a "probe photo" that is compared to over 80 million arrest photos, resulting in a list of ranked candidates as potential investigative leads.[265] Probe images used by law enforcement may be obtained from prior booking photos, driver's licenses, public social media accounts, public websites, cell phones, CCTV stills, electronic surveillance, and photos maintained by law enforcement partners.[266]

According to the FBI 2025 President's Budget Request:

> The NGI IPS' investigative FR search component allows authorized Federal, State, local, territorial, and Tribal law enforcement agencies to submit investigative face photos (probe photos) for an automated FR search of the NGI IPS…The automated NGI IPS FR algorithm is applied to each of the submitted images to determine if the image is of sufficient quality

[261] Ibid.
[262] DOJ Statement, at 6.
[263] Congressional Research Services, *Federal Law Enforcement Use of Facial Recognition Technology,* Oct. 27, 2020, https://crsreports.congress.gov/product/pdf/R/R46586.
[264] Federal Bureau of Investigation, "Next Generation Identification (NGI)," https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/biometrics/next-generation-identification-ngi (accessed Feb. 12, 2024).
[265] DOJ Statement, at 6.
[266] U.S. Dep't of Justice, DOJ Responses to U.S. Commission on Civil Rights Interrogatories, Mar. 26, 2024.

> for searching. If so, the FR algorithm creates a face template. Contributors receive a minimum of two, a maximum of 50, or default of 20 candidates returned in a ranked investigative candidate list. Contributors are also required to compare all available candidates against their probe photo(s).
>
> CJIS Systems Agency/State Identification Bureau must ensure all authorized law enforcement agencies take approved training prior to conducting investigative FR searches of the NGI IPS. In addition, FBI policies and procedures emphasize photo candidates returned are not to be considered "positive identifications." Further investigation must be performed before making an arrest. In FY 2023, 34,014 investigative FR searches of the NGI IPS had been performed.[267]

In May 2016, the U.S. Senate's Subcommittee on Privacy, Technology and the Law asked GAO to investigate how the FBI operates its NGI-IPS.[268] GAO evaluated the FBI's facial recognition capabilities, the extent to which the FBI was complying with privacy laws, and how the FBI assessed the accuracy of its facial recognition systems.[269] The 2016 GAO report explained that in 2008, the FBI developed Privacy Impact Assessments (PIAs), but DOJ did not approve PIAs for facial recognition systems until seven years later in 2015—after the NGI-IPS and FACE systems underwent changes. GAO stated that "[t]he timely publishing of PIAs would provide the public with greater assurance that the FBI is evaluating risks to privacy when implementing systems."[270] GAO also determined that the FBI did not publish a legally required Systems of Records Notice (SORN)[271] for NGI-IPS until May 2016, even though the FBI had been using the system since 2011. GAO also found that the FBI failed to conduct sufficient testing on the NGI-IPS system and determine how often errors occurred in searches of certain sizes.[272]

GAO concluded that without conducting sufficient testing, the FBI could not verify if the technology was returning accurate candidate lists for criminal investigations. Likewise, GAO found that the FBI had neither tested the databases belonging to the Departments of State nor Defense, nor state systems that the agency utilized for criminal investigations.[273] GAO made six recommendations, including that:

> [T]he Attorney General determine why PIAs and a SORN were not published as required and implement corrective actions, and [] the FBI director [] conduct tests to verify that NGI-IPS is accurate and take steps to determine whether systems used by external partners are sufficiently accurate for FBI's use. DOJ agreed with one, partially agreed with two, and

---

[267] U.S. Dep't of Justice Federal Bureau of Investigation, *FY 2025 President's Budget Request,* Mar. 2024, https://www.justice.gov/d9/2024-03/fbi_fy_2025_presidents_budget_narrative_3-5-24_final_1.pdf.
[268] U.S. Government Accountability Office, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, May 2016, https://www.gao.gov/assets/gao-16-267.pdf.
[269] Ibid.
[270] Ibid.
[271] The Privacy Act of 1974 requires agencies to publish a SORN in the Federal Register identifying the categories of individuals whose information is in the system of records, and the type of data collected. *See* 5 U.S.C. 552a(e)(4)(B).
[272] U.S. Government Accountability Office, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, May 2016, https://www.gao.gov/assets/gao-16-267.pdf.
[273] Ibid.

> disagreed with three of the six recommendations. In response, GAO clarified one recommendation, updated another recommendation, and continues to believe that all six recommendations remain valid. . .[274]

In June 2019, GAO issued a follow-up to its May 2016 report that assessed the actions the DOJ and FBI took in response to the 2016 recommendations.[275] The 2019 report found that the DOJ/FBI took action on only three of the six recommended actions in the 2016 report.[276] Specifically, GAO recommended that the agency publish certain privacy documents concerning its facial recognition systems, including updating its PIAs and publishing a SORN. The 2019 report found that the FBI had made some updates to its PIA process but had not acted on the SORN. Additionally, GAO made recommendations with respect to testing the accuracy of the FBI's FRT before using it, testing the accuracy on different list sizes, and testing the systems operated by partner agencies and states. GAO found that the agency had not made any progress on these recommendations.[277] Finally, GAO recommended that the DOJ and FBI conduct regular audits to determine if users were complying with their policies when using FRT to conduct searches. GAO was able to determine that the DOJ and FBI actions satisfied the intent of the recommendation, and it was closed as implemented.[278]

FACE Services

Located within the FBI's Investigative Services Support Unit is the Facial Analysis, Comparison and Evaluation (FACE) Services team – which provides additional support for FBI investigations.[279] FACE Operations Services uses the NGI-IPS database in combination with a number of other databases owned by the State Department and Department of Defense as well as many state-owned databases and facial recognition systems. Once the system provides the list of possible candidates, trained facial recognition examiners conduct a manual multi-level review of all the photos before returning any likely candidates to the FBI investigators.[280] FBI policies and procedures emphasize that photo candidates returned to FBI investigators are not to be considered positive identifications and further investigation must be performed before taking law enforcement action.[281]

The NGI data, including the photos in the NGI-IPS, are retained in accordance with the applicable retention schedule approved by the National Archives and Records Administration (NARA).[282] NARA approved the destruction of fingerprints and associated biometric and biographic information

---

[274] Ibid.
[275] U.S. Government Accountability Office, *Face Recognition Technology DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains*, Jun. 2019, https://www.gao.gov/assets/gao-19-579t.pdf.
[276] Ibid.
[277] Ibid.
[278] Ibid.
[279] Ibid.
[280] Ibid.
[281] DOJ, Affected Agency Review, Jun. 21, 2024.
[282] Federal Bureau of Investigation, *Privacy Impact Assessment for the [Next Generation Identification-Interstate Photo System],* Approved Oct. 2019, https://www.fbi.gov/file-repository/pia-ngi-interstate-photo-system.pdf.

when subjects attain 110 years of age or seven years after notification of death with biometric confirmation, however, criminal history records and transaction logs are permanently retained.[283]

According to DOJ:

> The FBI's Facial Analysis Comparison Evaluation (FACE) Operations Services supports authorized FBI assessments and investigations by enabling FBI personnel to submit requests for FR [facial recognition] searches of FBI's NGI-IPS as well as FRT systems maintained by 17 state agencies and 2 other federal agencies[284] with which the FBI has entered a MOU [Memoranda of Understanding]. Except for one state agency FRT system and one federal agency FRT system, FACE Operations Services personnel do not have direct login access—they only transmit requests to the applicable agencies who run the searches and return results, if any, back to FACE Operations Services.
>
> All FRT use cases are reviewed by the FBI's Science and Technology Branch, Office of the General Counsel—including the Privacy and Civil Liberties Officer, and Office of the Chief Information Officer—including the AI Ethics Council. FBI users must obtain supervisory approval and complete training in facial comparison and identification before accessing and using any FRT service. The FBI's policies and procedures emphasize that photo candidates returned are not to be considered positive identifications but treated simply as leads.[285]

The FBI's CJIS Audit Unit conducts audits of all federal and state agencies that access the NGI-IPS on a triennial basis.[286] The audit process includes: in-person and/or teleconference interviews with audit participant personnel; surveys and questionnaires completed by the audit participant; review of policy and procedural documents to include standard operating procedures, statutes, administrative rules, and forms; review of case files and/or other documentation associated with system transactions or access; demonstrations by the audit participant of administrative processes and information technology platforms; and exit briefings with audit participants to provide tentative results and potential areas of concern.[287]

DOJ wrote that in February 2024 the latest NIST FRTE report found the accuracy of the current FBI algorithm for its NGI-IPS exceeded 99.88 percent when comparing a probe photo to a gallery of arrest photos and exceeded 99.25 percent when searching webcam images against arrest photos.[288] Additionally, DOJ indicated that the FBI has considered other research partners' results, such as the 2023 United Kingdom National Physical Lab Report on FRT performance and other federally funded

---

[283] Ibid.
[284] Department of Defense and Department of State. Ibid.
[285] DOJ Statement, at 6.
[286] Federal Bureau of Investigation, *Privacy Impact Assessment for the [Next Generation Identification-Interstate Photo System],* Approved Oct. 2019, https://www.fbi.gov/file-repository/pia-ngi-interstate-photo-system.pdf.
[287] DOJ explained to the Commission that results of audits are not made public unless in response to a FOIA request or in instances in which the audit participant releases them. DOJ, Affected Agency Review, Jun. 21, 2024.
[288] DOJ Statement, at 8.

academic research and efforts performed internally.[289] DOJ did not provide the accuracy rates for various demographic groups.

The Department stated that the FBI CJIS Division has found no evidence of other federal, state, or local partners violating DOJ policies related to direct or indirect access to DOJ's facial recognition technology.[290]

USMS

The U.S. Marshals Service (USMS) uses FRT during fugitive, missing child, substantive criminal investigations, and protective security missions. DOJ wrote to the Commission that FRT is used solely to generate leads and not for positive identification.[291] According to DOJ, USMS has held a contract with Clearview AI for several years, and more recently, it has executed an MOU allowing it to access DHS's Homeland Security Information Network (HSIN) and request indirect facial recognition searches through state and local entities, such as fusion centers.[292] Because of the structure of USMS Task Force operations, which involves state and local law enforcement officers who are specially deputized as Task Force Officers (TFOs), these officers may also have access to FRT systems owned by the federal agency or other technology systems.[293] In circumstances where there is a demonstrated need for information, FRT systems may be accessed by TFOs following verification of their state/local law enforcement credentials.[294] Task Force Officers working on Task Forces with the FBI, DEA, and ATF may also have access to FRT systems owned or maintained by their respective parent agency.[295] In these instances, however, the Justice Department and its law enforcement components generally do not have direct access to state and local law enforcement agencies' FRT systems. In rare exceptions where a DOJ agency has a formal agreement allowing access to a state or local FRT system, DOJ employees accessing those systems are still bound by all relevant DOJ policies.[296]

In February 2023, the Marshals Service implemented a training requirement for staff using facial recognition services. Specifically, staff must complete Clearview AI's virtual training session prior to initially using the service, and complete Clearview AI's refresher training annually.[297] The Marshals Service officials stated that this training, which is about four hours in length, provides an overview of the functions of Clearview AI.[298] The Marshals Service had also taken steps to limit the

---

[289] Ibid.
[290] U.S. Dep't of Justice, DOJ Responses to U.S. Commission on Civil Rights Interrogatories, Mar. 26, 2024.
[291] DOJ Statement, at 7.
[292] Ibid., at 7. Fusion Centers are state-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between State, Local, Tribal and Territorial (SLTT), federal and private sector partners.
U.S. Dep't of Homeland Security, "Fusion Centers," https://www.dhs.gov/fusion-centers (accessed Mar. 29, 2024).
[293] DOJ Statement, at 7.
[294] Ibid.
[295] DOJ Affected Agency Review, Jun. 21, 2024.
[296] Ibid.
[297] U.S. Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties,* Sept. 2023, https://www.gao.gov/products/gao-23-105607.
[298] Ibid.

number of staff who use the service by requesting Clearview AI suspend the accounts of staff who were no longer using it or did not need to use the service, reducing the number of staff with active accounts from 103 to three.[299] As of July 2024, four staff with access to Clearview AI had completed the required training.[300] At the Commission's March 2024 briefing, Clearview AI founder and CEO Hoan Ton-That stated that since early 2020 the company has had a mandatory training requirement for all users.[301]

DOJ's interim FRT policy and the FBI's policy prohibit the use of FRT results as a means of positive identification as the sole basis for enforcement action. Instead, FRT results generate investigative leads that require further investigation to substantiate or invalidate those leads.[302] The possible issues with using FRT for lead generation are discussed below.

In May 2022, President Biden issued Executive Order (E.O.) 14074, which directed DOJ to contract with the National Academy of Sciences to:

> (i) conduct a study of facial recognition technology, other technologies using biometric information, and predictive algorithms, with a particular focus on the use of such technologies and algorithms by law enforcement, that includes an assessment of how such technologies and algorithms are used, and any privacy, civil rights, civil liberties, accuracy, or disparate impact concerns raised by those technologies and algorithms or their manner of use; and
>
> (ii) publish a report detailing the findings of that study, as well as any recommendations for the use of or for restrictions on facial recognition technologies, other technologies using biometric information, and predictive algorithms by law enforcement.[303]

By April 2023, DOJ officials told GAO that although they had developed a department-wide facial recognition draft policy, they intended to wait for the efforts required by E.O. 14074 to be complete before issuing.[304] In September 2023, GAO reported:

> DOJ officials told us that they had identified funding to address the requirement to develop a study on facial recognition technology but had not yet awarded the funding to the National Academy of Sciences. The executive order called on DOJ to enter into the contract by November 2022, and it had not done so as of April 2023. Additionally, the executive order called on the interagency effort to issue a report—using the results of the National Academy

---

[299] Ibid.
[300] DOJ, Affected Agency Review, Jun. 21, 2024.
[301] Ton-That Testimony, p. 60.
[302] Ibid., at 19.
[303] Exec. Order No. 14074, *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety*, May 25, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/05/25/executive-order-on-advancing-effective-accountable-policing-and-criminal-justice-practices-to-enhance-public-trust-and-public-safety/
[304] U.S. Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties,* Sept. 2023, https://www.gao.gov/products/gao-23-105607.

> of Sciences study—by November 2023. However, as of April 2023, the funding for the study had not yet been awarded, the study had not yet begun, and it is unclear what impact this may have on DOJ's ability to issue their facial recognition policy in a timely manner.[305]

As of April 2023, the DOJ's National Institute of Justice (NIJ) was undertaking administrative tasks prior to awarding funding for the study,[306] rendering a delay in the National Academy of Science study. The National Academies report was published in January 2024,[307] and its recommendations are discussed in Chapter 3.[308]

Since the signing of E.O. 14074 the agency has worked on more than 90 deliverables, established the National Law Enforcement Accountability Database, and has created accreditation standards to encourage law enforcement agencies to adopt policies consistent with the Executive Order.[309]

In January 2024, 18 senators requested information from the Justice Department regarding the funding and oversight of facial recognition and other biometric technologies under the Civil Rights Act of 1964 and other applicable federal statutes and regulations.[310] The letter asked a series of questions about the extent to which federal grant recipients using FRT were complying with federal civil rights laws; whether DOJ has any policies or trainings in place regarding FRT use and Fourth Amendment protections; and what practices or policies DOJ has to ensure its programs audit new biometric technologies, engage in proper oversight of their deployment, and did not violate any relevant constitutional or statutory civil rights protections.[311] The senators asked for the questions to be addressed by February 29, 2024.[312] As of the writing of this report, the Commission cannot confirm any response by DOJ to the letter.

In addition to federal law enforcement use of FRT, according to public records, DOJ has awarded at least $3.2 million to local law enforcement agencies for facial recognition software since 2007.[313] In the Department's response to the Commission's inquiries, DOJ indicated that the Office of Justice Programs' (OJP) BJA has provided grant awards where recipients and/or subrecipients have used

---

[305] Ibid.
[306] Ibid.
The DOJ explained to the Commission that since the NAS study on FRT was already ongoing, the Department decided that the NIJ-sponsored study should focus narrowly on DNA biometrics and predictive algorithms, not FRT. U.S. Dep't of Justice, Affected Agency Review, Jun. 21, 2024.
[307] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.
[308] *See infra* note 654.
[309] U.S. Dep't of Justice, "Department of Justice Fact Sheet on Implementing Executive Order on Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety," Updated May 24, 2024, https://www.justice.gov/olp/department-justice-fact-sheet-implementing-executive-order-advancing-effective-accountable.
[310] Letter to Attorney General Merrick Garland, "Re: Facial Recognition and Title VI," Jan. 18, 2024, https://www.warnock.senate.gov/wp-content/uploads/2024/01/1.18.24-Letter-to-DOJ-re-Facial-Recognition-and-Title-VI.pdf.
[311] Ibid.
[312] Ibid.
[313] Alfred Ng, "Washington takes aim at facial recognition," *Politico,* Jan. 19, 2024, https://www.politico.com/news/2024/01/19/washington-takes-aim-at-facial-recognition-00136498.

funding for facial recognition technology.[314] For example, OJP identified 12 individual grant awards/subawards totaling $721,755 under the Edward Byrne Memorial Justice Assistance Grant (JAG) Program for fiscal years 2021-2023 that did, at least partially, fund the purchase or installation of FRT.[315] BJA includes an award condition for JAG awards on the "Use of Funds for Facial Recognition Technology" that reads:

> In accepting this award, the recipient agrees that grant funds cannot be used for Facial Recognition Technology (FRT) unless the recipient has policies and procedures in place to ensure that the FRT will be utilized in an appropriate and responsible manner that promotes public safety, and protects privacy, civil rights, and civil liberties and complies with all applicable provisions of the U.S. Constitution, including the Fourth Amendment's protection against unreasonable searches and seizures and the First Amendment's freedom of association and speech, as well as other laws and regulations. Recipients utilizing funds for FRT must make such policies and procedures available to DOJ upon request.[316]

DOJ stated every applicant for federal financial assistance must sign a Title VI assurance and must agree to comply with the nondiscrimination provision as a condition of receiving funding.[317]

Emerging Civil Rights Concerns

A September 2023 GAO report examining federal law enforcement use of FRT reported that, at the time of the report, four of the seven agencies reviewed did not have guidance or policies specific to FRT that addressed civil rights and civil liberties.[318] The report stated that FBI officials told key internal stakeholders that certain staff must take training to use a facial recognition service. However, in practice, the FBI only recommended it as a best practice.[319] GAO found that few of these staff completed the training; across the FBI, only 10 of 196 staff who accessed facial recognition services completed facial recognition training.[320] The FBI implemented a training requirement for all staff in December 2023.[321]

---

[314] U.S. Dep't of Justice, DOJ Response to U.S. Commission on Civil Rights Interrogatories, Mar. 26, 2024.
[315] Ibid.
[316] U.S. Dep't of Justice, DOJ Response to U.S. Commission on Civil Rights Interrogatories, Mar. 26, 2024.
[317] The Justice Department explained to the Commission that OJP's Office for Civil Rights (OCR) ensures that recipients of federal financial assistance from the Department comply with Title VI and Title VI regulations through several oversight activities. OCR receives complaints from individuals or groups who believe they have experienced discrimination under the laws that OCR enforces, including Title VI, and evaluates each complaint to determine whether the office has jurisdiction over the complaint and whether the complaint provides enough information to establish an initial claim of discrimination. Generally, the Department issues public statements when there has been a finding of nondiscrimination or obtains a resolution of an investigation. DOJ Agency Affected Review, Jun. 21, 2024.
[318] Gretta Goodwin, Director, Homeland Security and Justice, U.S. Government Accountability Office, Written Statement for the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, at 5 (hereinafter Goodwin Statement).
[319] U.S. Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties,* Sept. 2023, https://www.gao.gov/products/gao-23-105607.
[320] Ibid.
[321] DOJ Agency Affected Review, Jun. 21, 2024.

Since the FBI permits facial recognition in general support of investigations or assessments,[322] the Center for Democracy & Technology explained that:

> [N]ot only are FBI personnel allowed to conduct facial recognition scans of individuals who are not designated criminal suspects, they can conduct scans as part of assessments when there is not even a factual predicate for criminal wrongdoing. Using facial recognition in this manner creates serious risk of fishing investigations, disparate treatment, and outright abuse.[323]

Clare Garvie of the National Association of Criminal Defense Lawyers testified to the Commission that FRT use in a law enforcement context risks entrenching historical patterns of over-policing in minority neighborhoods.[324] She wrote that "[s]ome of the most controversial, high-risk pilot facial surveillance programs have occurred in cities with non-White populations well above the national average."[325] Additionally, because many police FRT systems, including the FBI's NGI-IPS, use arrest databases, they are pulling from a dataset reflective of "racial and other biases present in both historic and current arrest rates."[326] FRT misidentification by law enforcement can have substantive ramifications. Nicol Turner Lee of the Brookings Institution testified that "we're not talking about…facial recognition in a healthcare scenario…we're talking about the fact that people of color are more likely to be arrested."[327]

Suggesting that FRT is only used as an investigative lead can downplay the consequences that can occur if a law enforcement investigation misidentifies someone. At the Commission's briefing, Garvie testified that while using FRT only as an investigative lead is valuable in theory, it is unclear exactly what is meant by the term "lead."[328] Garvie explained that there are often two assumptions underlying use of FRT searches: one, they are a reliable means of identification, and two, because they are generating investigative leads (as opposed to probable cause for arrest), there is not a requirement to disclose the usage of FRT to the defense.[329] She declared it a "trust, but don't verify" approach to policing.[330]

However, when using high-performing algorithms combined with trained personnel, FRT can be an extremely useful tool for law enforcement investigations. For instance, Hoan Ton-That CEO of Clearview testified to an example where the use of FRT helped to solve a child exploitation case.

---

[322] Facial Recognition Technology (Part II): Ensuring Transparency in Government Use: Hearing before the House Committee on Oversight, 116th Cong. (June 4, 2019) (statement by Kimberly Del Greco, Deputy Assistant Director, FBI Criminal Justice Information Services Division), https://perma.cc/7NEW-RRW9.
[323] Center for Democracy & Technology, "Transparency and Policy Recommendations for Federal Law Enforcement Use of Facial Recognition," Jan. 19, 2024, https://cdt.org/wp-content/uploads/2024/01/DOJ-DHS-Comment-Transparency-and-Policy-Recommendations-for-Federal-Law-Enforcement-Use-of-Facial-Recognition.pdf.
[324] Garvie Statement, at 2.
[325] Ibid.
[326] Ibid., at 3.
[327] Turner Lee Testimony, p. 178.
[328] Garvie Testimony, p. 235.
[329] Garvie Statement, at 6.
[330] Ibid.

Ton-That explained that investigators could not locate the suspect but gained clues through the use of Clearview AI's photo database.

> From those two clues, they were able to talk to the [man's] employer, find the name, and get further evidence to get a search warrant. They found thousands more images and videos of child exploitation on the suspect's device. Today, this man is doing 35 years in jail, and they were able to save a 7-year-old girl.[331]

Jake Parker of the Security Industry Association explained in his statement to the Commission the importance of understanding the investigatory use of FRT in context:

> Other non-technological methods are also routinely used to search for leads starting from the same type of available image, such as manually looking through arrest photos, making public announcements or soliciting anonymous tips. Any leads that result must be confirmed independently in the same manner.[332]

Chief Armando Aguilar of the Miami Police Department explained that maintaining public safety depends on establishing community trust, and the use of FRT can help build that trust. Aguilar explained that:

> Violent crime, especially unsolved violent crime, is among the greatest threats that serve to undermine that trust. For example, a shooting takes place. A community member calls our anonymous tip line and gives us the shooter's name. Absent any other evidence to support the tip, the investigation goes cold. People stop reporting gunfire and the police in turn do not respond to gunfire that we do not know about.
>
> The perception among the community is that the police are at best unable to keep them safe or at worst unwilling to. Artificial intelligence helps bridge that gap by allowing law enforcement to solve and prevent crime and to protect our most vulnerable communities.[333]

Civil rights advocates maintain that for FRT to be trusted, there needs to be transparency and oversight to ensure that an individual's rights are not violated during the course of an investigation, regardless of criminality.[334]

In addition to the lack of operational testing of FRT systems,[335] there remains a lack of clear quantifiable evidence regarding the benefits of FRT use in law enforcement. There are many anecdotes about successful use cases provided by FRT developers,[336] news outlets,[337] public

---

[331] Ton-That Testimony, pp. 29-30.
[332] Security Industry Association, Public Comment, Apr. 8, 2024 [on file].
[333] Aguilar Testimony, p. 36.
[334] *See e.g.,* Kinsey Testimony, p. 52; Mina Testimony, p. 98; MacCleery Testimony, pp. 152, 172-73.
[335] *See, supra* notes 245-254.
[336] Ton-That Testimony, pp. 29-32.
[337] Dyllan Furness, "Police used facial recognition software to identify the Capital Gazette shooter," *Digital Trends,* Jun. 29, 2018, https://www.digitaltrends.com/cool-tech/capital-gazzette-shooter-facial-recognition/; Ryan J. Reilly, "FBI arrests Jan. rioter IDed with help of facial recognition and a throwback Eagles hat," *NBC News,* Jan. 31, 2024,

defenders,[338] and law enforcement officials themselves.[339] Yet a comprehensive assessment of the successful implementation and use of FRT has yet to be conducted. Katie Kinsey, Chief of Staff at NYU Law's Policing Project, testified that:

> In the absence of adequate transparency and testing, we have no idea if these handful of success stories represent the tip of the iceberg or the entire story. And the government should not be investing public resources in facial recognition—and risking individuals' civil rights and liberties—if it cannot gauge the expected benefits of use.[340]

While FRT can be beneficial to law enforcement and public safety, the federal government should work to ensure the process is as transparent as possible, particularly when the technologies are being purchased with federal funds.

Agency Efforts

In its September 2023 report, GAO made two recommendations to the FBI related to training for facial recognition services,[341] and two recommendations to DOJ related to privacy requirements.[342] DOJ concurred with the recommendations. As of May 2024, the training recommendations directed to the FBI have been implemented and the privacy recommendations remain open, although some agencies in the Department[343] have begun to address outstanding privacy requirements identified during the GAO review.[344]

According to written testimony from DOJ, in February 2022 the Department launched an FRT Working Group that met regularly throughout 2022 and 2023, tasked with developing an interim FRT policy.[345] DOJ indicated that the interim policy, announced December 2023, is consistent with

---

https://www.nbcnews.com/politics/justice-department/fbi-arrests-jan-6-rioter-facial-recognition-philadelphia-eagles-hat-rcna136589.

[338] Kashmir Hill, "Clearview AI, Used by Police to Find Criminals, Is Now in Public Defenders' Hands," *The New York Times,* Sep. 18, 2022, https://www.nytimes.com/2022/09/18/technology/facial-recognition-clearview-ai.html.

[339] Aguilar Testimony, pp. 34-40.

[340] Kinsey Statement, p. 7.

[341] "The Director of the FBI should clarify the status of its training requirement for staff using Clearview AI to FBI's AI Ethics Council and the Privacy and Civil Liberties Unit," and "The Director of the FBI should implement a training requirement for staff using facial recognition services to support criminal investigations."
U.S. Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties,* Sept. 2023, https://www.gao.gov/products/gao-23-105607.

[342] "The Attorney General should ensure the Chief Privacy and Civil Liberties Officer works with DOJ components continuing to use facial recognition services to address outstanding privacy requirements, and update privacy documentation as appropriate," and "The Attorney General should ensure the Chief Privacy and Civil Liberties Officer collaborates with component program, acquisition, and privacy officials to evaluate components' adherence to the department's privacy compliance process for facial recognition services—taking into account the results of this report—and to remediate any deficiencies identified during their evaluation." *See* U.S. Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties,* Sept. 2023, https://www.gao.gov/products/gao-23-105607.

[343] The U.S. Marshals Service finalized an initial privacy assessment for a facial recognition service. *See* Goodwin Statement, at 9.

[344] Goodwin Statement, at 8.

[345] DOJ Statement, at 1-2.

recommendations from the GAO 2023 report. DOJ stated that the policy will, among other things, "require each component that uses facial recognition systems to develop and implement training and qualification requirements, as applicable, tailored to that component's missions."[346]

As of May 1, 2024, the interim policy has not yet been made public, but DOJ submitted it upon request to the Commission for review. The policy mandates that components using FRT systems must develop and implement training and qualification requirement, and that department personnel using FRT systems must be trained on relevant legal and policy requirements. For example, the Department plans to provide recorded training for Assistant U.S. Attorneys and others in U.S. Attorney's offices.[347]

DOJ also stated that only qualified personnel who have completed these requirements may use or approve FRT systems.[348]

DOJ indicated the interim policy "prohibits unlawful use of FRT, provides guardrails to ensure effective and compliant use, and addresses the Department's FRT governance structure, including scope of FRT use, implementation, procurement, training, protection of privacy and civil rights, accuracy, the approval process for FRT use, accounting and reporting, and data retention."[349] As applied:

> All photos collected and used by the FBI must be collected pursuant to the Attorney General's Guidelines for the FBI's Domestic Operations (AGG DOM) and the FBI's Domestic Investigations and Operations Guide (DIOG). The FBI's use of FRT during an investigation must have a valid purpose consistent with the AGG-DOM and must comply with the U.S. Constitution and all applicable statutes, Executive Orders, and Department of Justice (DOJ) regulations and policies. Additionally, the use of FRT, generally, is subject to Section 208 of the E-Government Act, and certain information acquired or generated attendant to use of FRT is governed by the Privacy Act of 1974.[350]

The policy mandates that systems be assessed for accuracy across demographic groups, that personnel using or approving FRT must receive required training, and that activity protected by the First Amendment not be the sole basis for the use of FRT.[351]

DOJ stated:

> The Interim FRT Policy requires that Department FRT systems be assessed for risk to accuracy across demographic groups, bias, and unlawful discrimination; that personnel using or approving FRT systems must receive required training on relevant legal and policy requirements; and that mandated training must include at a minimum, the terms of the Interim

[346] Goodwin Statement, at 8.
[347] U.S. Dep't of Justice, DOJ Responses to U.S. Commission on Civil Rights Interrogatories, Mar. 26, 2024.
[348] Goodwin Statement, at 8.
[349] DOJ Statement, at 2.
[350] U.S. Dep't of Justice, DOJ Response to U.S. Commission on Civil Rights Interrogatories, Mar. 26, 2024.
[351] DOJ Statement, at 2-3.

> FRT Policy, the mandates of relevant privacy, civil rights, and civil liberties laws, and discussion of discovery obligations related to FRT use.
>
> Notably, the Interim FRT Policy mandates that activity protected by the First Amendment may not be the sole basis for the use of FRT. This would include peaceful protests and lawful assemblies, or the lawful exercise of other rights secured by the Constitution and laws of the United States. Additionally, under this policy pursuant to the Department's anti-discrimination policies and other anti-discrimination laws, Department personnel "shall never use FRT to engage in or facilitate unlawful discriminatory conduct."[352]

In February 2024, DOJ announced the Department's first Chief Science and Technology Advisor and Chief Artificial Intelligence (AI) Officer, Jonathan Mayer, assistant professor at Princeton University's Department of Computer Science and School of Public and International Affairs.[353] Attorney General Garland stated:

> The Justice Department must keep pace with rapidly evolving scientific and technological developments in order to fulfill our mission to uphold the rule of law, keep our country safe, and protect civil rights. Jonathan's expertise will be invaluable in ensuring that the entire Justice Department—including our law enforcement components, litigating components, grantmaking entities, and U.S. Attorneys' Offices—is prepared for both the challenges and opportunities that new technologies present.[354]

The Chief AI Officer chairs the Emerging Technology Board (ETB), which has been tasked to implement relevant Executive Orders, support coordination and governance of AI across DOJ, provide guidance to leadership, and advance information sharing across the department relevant to emerging technology best practices and use cases.[355]

While multiple lawmakers have proposed potential regulations for FRT,[356] there are currently no federal regulations dictating DOJ's usage of the technology.[357] The Commission requested several representatives from DOJ to participate in the Commission's March 2024 briefing.[358] DOJ provided a written statement to the Commission in lieu of providing public testimony.[359]

---

[352] U.S. Dep't of Justice, DOJ Response to U.S. Commission on Civil Rights Interrogatories, Mar. 26, 2024.
[353] U.S. Department of Justice, "Attorney General Merrick B. Garland Designates Jonathan Mayer to Serve as the Justice Department's First Chief Science and Technology Advisor and Chief AI Officer," Feb. 22, 2024, https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-designates-jonathan-mayer-serve-justice-departments-first.
[354] Ibid.
[355] DOJ Statement, at 4.
[356] *See infra,* notes.627-646.
[357] Alfred Ng, "Washington takes aim at facial recognition," *Politico,* Jan. 19, 2024, https://www.politico.com/news/2024/01/19/washington-takes-aim-at-facial-recognition-00136498.
[358] *See* Commissioner Mondaire Jones, testimony, *Facial Recognition Technology Briefing,* p. 12.
[359] DOJ Statement.

U.S. Department of Homeland Security (DHS)

Congress established DHS as a federal executive agency with broad duties and authorities, as part of the Homeland Security Act of 2002.[360] DHS was created in response to 9/11, and its mission is to prevent terrorism and other homeland security threats, as well as to "carry out all the functions of entities transferred to the Department [such as FEMA, USSS and FPS]."[361] The Act relocated and reorganized several federal agencies, such as the U.S. Customs Service (USCS) and the Immigration and Naturalization Service (INS), respectively formerly agencies of the Department of the Treasury and the DOJ, under the umbrella of DHS.[362] Further, the Act created the Transportation and Security Administration (TSA) and Immigrations and Customs Enforcement (ICE). The Department, including all of its agencies, must "ensure that the civil rights and civil liberties of persons are not diminished by efforts, activities, and programs aimed at securing the homeland."[363] DHS is the third largest federal department (following the Departments of Defense and Veterans Affairs), and currently has "more than 260,000 employees in jobs that range from aviation and border security to emergency response, from cybersecurity analyst to chemical facility inspector."[364]

In addition to the authority to review nondiscrimination compliance of DHS funding recipients, Congress provided the DHS's CRCL broad jurisdiction to advise the DHS Secretary regarding all agency policies, to review complaints about civil rights matters, and to provide public information about them.[365] CRCL also has jurisdiction, or responsibility, to evaluate internal Department policy and actions for compliance with civil rights laws on behalf of the public.[366] Notwithstanding this broad jurisdiction with respect to Department programs, Congress did not assign this civil rights office authority to enforce its views of the law or to review policies before they are implemented.

Peter Mina, CRCL's Deputy Officer for Programs and Compliance, testified that as the DHS office responsible for civil rights and civil liberties enforcement, CRCL is responsible for providing "advice and oversight to the Department's efforts to ensure [facial recognition] technology works to reduce the potential for racial, ethnic, or gender bias and other types of discrimination. In addition, CRCL investigates complaints that include allegations of racial profiling or other impermissible bias."[367]

---

[360] 6 U.S.C. § 111(a); Pub. L. 107-296, Title I, § 101 (Nov. 25, 2002).
[361] 6 U.S.C. 111 (a).
[362] *See* 6 U.S.C. § 542 and accompanying Modification Plan (Nov. 25, 2002) and Reorganization Plan Modification (Jan. 30, 2003).
[363] *Id.* § 111(b)(1)(G).
[364] U.S. Dep't of Homeland Security, "About DHS," https://www.dhs.gov/about-dhs (accessed Mar. 29, 2024).
[365] U.S. Dep't of Homeland Security, "Office for Civil Rights and Civil Liberties," https://www.dhs.gov/office-civil-rights-and-civil-liberties.
[366] 6 U.S.C. § 111(a); Pub. L. 107-296, Title I, § 101 (Nov. 25, 2002).
[367] Mina Testimony, p. 89.

Many Americans associate the federal usage of FRT with the airport security run by TSA[368] (e.g., gate and bag screening) and Customs and Border Protection (CBP) (i.e., and immigration). Both agencies are housed under DHS.

CBP is "one of the world's largest law enforcement organizations and is charged with keeping terrorists and their weapons out of the United States while facilitating lawful international travel and trade."[369] CBP was formed on March 1, 2003. Prior to its establishment, security and compliance of international travel and trade were previously conducted by various agencies (e.g., TSA, the Coast Guard, and CBP).[370]

The Aviation and Transportation Security Act of 2001 created TSA on November 19, 2001.[371] Its mission is to "protect the nation's transportation systems to ensure freedom of movement for people and commerce." Like DHS, TSA was created in response to the 9/11 terrorist attacks.[372]

Like CBP, ICE was formed March 1, 2003 when DHS absorbed other federal agencies and programs.[373] Its mission statement is to "[p]rotect America through criminal investigation and enforcing immigration laws to preserve national security and public safety."[374] ICE has more than 20,000 law enforcement and support personnel with three operational directorates: Homeland Security Investigations (HSI), Enforcement and Removal Operations (ERO), and the Office of the Principal Legal Advisor (OPLA).[375] HSI special agents gather evidence to identify and build criminal cases against transnational criminal organizations, terrorist networks and facilitators, and "other criminal elements that threaten the United States."[376]

DHS does not have specific regulations regarding FRT's usage relating to civil rights. DHS CRCL is responsible for assisting the Department in developing, implementing, and periodically reviewing policies and procedures to ensure the protection of civil rights and civil liberties and that those protections are appropriately considered in all aspects of operations, including in programs using biometric technologies.[377] Department-wide policy dictates that all uses of face recognition and face capture technologies shall be thoroughly tested to ensure there is no unintended bias or disparate impact in accordance with national standards.[378] DHS will review all existing uses of this technology and conduct periodic testing and evaluation of all systems to meet performance goals. The policy

[368] DHS noted that TSA airport screening is not a law enforcement activity and is a different use case and context for FRT. DHS Affected Agency Review, Jun. 28, 2024.
[369] U.S. Dep't of Homeland Security, "About CBP," https://www.cbp.gov/about.
[370] U.S. Customs and Border Protection, "March 1, 2003: CBP is Born," Oct. 13, 2016, https://www.cbp.gov/about/history/march-1-2003-cbp-born.
[371] *See* Aviation and Transportation Security Act, P.L. No. 107-71 (2001).
[372] Transportation Security Administration, "Mission," https://www.tsa.gov/about/tsa-mission.
[373] U.S. Immigrations and Customs Enforcement, "History of ICE," https://www.ice.gov/features/history (accessed Apr. 8, 2024).
[374] U.S. Immigrations and Customs Enforcement, "Mission," https://www.ice.gov/mission (accessed Apr. 8, 2024).
[375] U.S. Immigrations and Customs Enforcement, "About ICE," https://www.ice.gov/about-ice (accessed Apr. 8, 2024).
[376] Ibid.
[377] DHS Affected Agency Review, Jun. 29, 2024.
[378] U.S. Dep't of Homeland Security, "DHS Announces New Policies and Measures Promoting Responsible Use of Artificial Intelligence," Sept. 14, 2023, https://www.dhs.gov/news/2023/09/14/dhs-announces-new-policies-and-measures-promoting-responsible-use-artificial.

also requires that U.S. citizens be afforded the right to opt-out of face recognition for specific, non-law enforcement uses, prohibits face recognition from being used as the sole basis of any law or civil enforcement related action, and establishes a process for Department oversight offices including CRCL, the Privacy Office, and the Office of the Chief Information Officer, to review all new uses of face recognition and face capture technologies.[379]

In addition, CRCL's role with respect to AI is the Responsible Use Group (RUG) established under DHS's AI Task Force (AITF) in April 2023.[380] According to the DHS webpage, the Responsible Use Group is led by the Officer for Civil Rights and Civil Liberties, Shoba Sivaprasad Wadhia. CRCL's role in this Task Force is to "provide guidance, risk assessment, mitigation strategies, and oversight for the protection of individual rights in projects championed by the DHS AI Task Force."[381]

According to DHS's website, the Responsible Use Group's goals include:

- Establishing a working and appropriately evolving definition of responsible use of AI at DHS.
- Engaging stakeholders, assessing risks, and prescribing tailored mitigation in each AITF-sponsored project.
- Working to advance the equitable use of AI by DHS through policies implementing AI-related authorities and requirements.
- Building a community of AI governance and common vocabulary around responsible use across DHS.
- Strengthening the DHS AI workforce through trainings and other learning opportunities focused on responsible use, trustworthiness, accountability, and strong governance practices.
- Capturing and using the Department's experience, best practices, and lessons learned regarding responsible use of AI.[382]

FRT Utilization

At the Commission's briefing, Peter Mina, Deputy Officer for Programs and Compliance with CRCL testified that "DHS uses biometrics such as fingerprints, iris and face recognition to enable operational missions, both to support national security and public safety and deliver benefits and services with greater efficiency and accuracy."[383] Arun Vemury, Senior Engineering Advisor for Biometrics and Identity Technologies with DHS S&T, explained that their work on biometric and identity technologies, including face recognition, applies deliberate and rigorous methodologies for research, test, and evaluation to inform the DHS components of specific technology capabilities and

[379] Ibid.
[380] Memorandum, Establishment of an Artificial Intelligence Task Force, April 20, 2023, https://www.dhs.gov/sites/default/files/2023-04/23_0420_sec_signed_ai_task_force_memo_508.pdf
[381] DHS, "Collaborative Governance," "Responsible Use Group," https://www.dhs.gov/ai/ensuring-ai-is-used-responsibly
[382] DHS, "Collaborative Governance," "Responsible Use Group," https://www.dhs.gov/ai/ensuring-ai-is-used-responsibly
[383] Mina Testimony, p. 86.

performance while adhering to privacy, civil rights, and civil liberties protections.[384] He testified that:

> Recent advances in artificial intelligence (AI) have enabled some commercial face recognition technologies to make dramatic gains in accuracy. These technologies now hold immense potential for enhancing the operational capabilities of DHS Components. However, realizing this potential in operations requires careful analysis and planning as performance of AI systems can be affected by multiple factors.[385]

Given DHS's broad scope and mission, several agencies housed within the Department utilize FRT and have established their own protocols (discussed below) but are still governed by the Department's Facial Recognition and Face Capture Directive on FRT use. This Directive was issued in September 2023 and

> establishes an enterprise policy for the authorized use of face recognition and face capture technologies by DHS. It applies the use of face recognition and face capture technologies for any purpose and limits the use of face analysis technology, including technologies used by federal, state, local, tribal, and territorial governments, non-U.S. governments, and international entities operated by or on behalf of the Department.[386]

U.S. Customs and Border Protection (CBP)

The implementation of biometric technology stems from the 9/11 Commission Report, in response to the need to prevent terrorist travel to the United States, recommending an automated system to record the arrivals and departures of visitors at all air, sea, and land ports of entry.[387] Now, CBP has implemented facial biometrics into the entry processes at all international airports and into the exit processes at 53 airports, as well as expanded facial biometrics at 40 seaports and all pedestrian lanes at the Southwest and Northern Border ports of entry.[388] CBP conducts biometric vetting using facial recognition for the following populations: (1) individuals seeking to enter or exit the United States whose names appear on a flight or vessel manifest, or voluntary manifests in the form of bus or rail manifests ("manifested travelers") as well as applicants for admission into the United States via air, sea, and land border pedestrian lanes; (2) individuals applying for CBP programs that facilitate travel to the United States; and (3) subjects of interest who require additional research and analysis.[389]

CBP has tested whether to build galleries using photos in a variety of settings, but this has not been implemented as a practice. In pedestrian entry/exit, CBP uses 1:1 matching, meaning a live photo is matched against the document photo.

---

[384] Vemury Statement, at 1.
[385] Ibid.
[386] Mina Testimony, p. 87.
[387] U.S. Customs and Border Protection, "Biometrics," https://www.cbp.gov/travel/biometrics (accessed Feb. 7, 2024).
[388] Ibid.
[389] *See* Department of Homeland Security Privacy Impact Assessment Update DHS/CBP/PIA-006(e) Automated Targeting System at 23-24; U.S. Dep't of Homeland Security, DHS Responses to U.S. Commission on Civil Rights Interrogatories, Apr. 17, 2024, at 4.

The technology used, known as the Traveler Verification Service (TVS), begins when travelers presents themselves for entry or exit and encounter a camera connected to CBP's cloud-based TVS facial matching service via a secure, encrypted connection.[390] The camera matches live images with existing photo templates from the passenger's travel documents.[391] Once the camera captures a quality image and the system can successfully match it with historical photo templates of all travelers from the set of photos associated with that traveler's documents and declarations, the traveler proceeds to inspection for admissibility by a CBP officer or exits the United States.[392] As of January 30, 2024, CBP has 238 airports using Biometric Facial Comparison Technology in the air entry environment, including all 14 CBP Preclearance locations and 53[393] locations for air exit (international departures).[394]

In her written statement to the Commission, Diane Sabatino, Acting Executive Assistant Commissioner of CBP's Office of Field Operations, stated that in its latest NIST testing results, the NEC algorithm used by CBP had the highest performance evaluation in the 1:many identification tests, with an accuracy rate of 99.88 percent.[395] In her testimony, she stated that CBP analysts have performed operational analytics on TVS matching, showing

> a negligible effect in regard to biometric matching based on country of citizenship, age, or gender while achieving an average technical match of 99.4 percent on entry and 98.1 percent on exit. Technical match rates remain high among citizens from various regions of the globe: Africa 99.5 percent match rate; Asia 99.3 percent match rate; Central America 99.6 percent match rate; and Europe 99.6 percent match rate.[396]

In total, as of June 4, 2024, more than 532 million travelers have been processed using biometric facial comparison technology, allowing CBP to confirm more than 1,990 individuals posing under a false or assumed identity and over 358,000 overstays through biometric exit.[397]

Transportation Security Administration (TSA)

One way in which TSA is using facial identification to verify a passenger's identity at security checkpoints is by using CBP's TVS, which creates a secure biometric template of a passenger's live facial image taken at the checkpoint and matches it against a gallery of templates of pre-staged photos within TVS, limited solely to passengers traveling from the airport that day who have similarly chosen to participate. The photographs in the gallery are sourced from photographs that have previously provided to the government (e.g., in the form of a U.S. passport or visa). Participation is limited to DHS Trusted Travelers (TSA PreCheck® and CBP Global Entry). According to TSA, this

[390] U.S. Customs and Border Protection, "Biometrics," https://www.cbp.gov/travel/biometrics (accessed Feb. 7, 2024).
[391] Ibid.
[392] Ibid.
[393] Updated number provided by DHS Affected Agency Review, Jun. 28, 2024.
[394] U.S. Customs and Border Protection, "Airports | CBP Biometrics," https://www.cbp.gov/travel/biometrics/airports (accessed Feb. 8, 2024).
[395] Sabatino Statement, at 1.
[396] Ibid., at 1-2.
[397] DHS Affected Agency Review, Jun. 28, 2024.

is an optional process for passengers, who may opt out of the process at any time and instead choose the standard identity verification by a Transportation Security Officer (TSO).[398] TSA and CBP are also allowing airport and airline partners to request the use of TVS for identity verification under an established TSA process outlined in 49 U.S.C. § 114.1. These partners purchase camera equipment in order to take photos of voluntary passengers at airport baggage drop and boarding locations for transmission to TVS, which creates biometric templates of these photos and compares them against templates of existing DHS holdings.[399] This process is optional and only available at a time and place where travelers are already required to verify identity.

Outside of performance testing, TSA does not retain a copy of the passenger's live photograph taken at the TSA checkpoint because it is overwritten as soon as the next passenger in line has a live photograph captured. During operational testing, however, TSA may retain these live photographs during limited periods of field demonstration data collection efforts by DHS S&T under tightly constrained terms and limits.[400] For performance testing, TSA collects a live photograph of the passenger, passport number, known traveler number, transactional metadata (e.g., transaction ID, timestamps, quality scores), and the match results.[401] TSA then converts the information into an anonymized format, encrypts it, and transfers it for temporary analysis to DHS S&T, which assesses the effectiveness of this biometric field demonstration, and DHS S&T deletes the data within 180 days pursuant to a MOU between TSA and DHS S&T in accordance with the National Archives Records Administration approved records management policies and dispositions schedules.[402]

According to testimony received from DHS, at airports where TSA has deployed its FRT, a passenger may decline to have a photo taken to verify their identity, and they will undergo manual verification by the TSO.[403] Jason Lim, Identity Management Capability Manager for TSA, wrote to the Commission that:

> TSA uses second-generation Credential Authentication Technology (CAT-2) scanners as travelers enter the screening process. The first station, called the traveler document checker or TDC, is where the traveler's identity is verified before moving into the physical screening process. CAT-2s assist our TSOs in verifying the authenticity of a traveler's ID credential, as well as their flight information and vetting status. CAT-2 technology allows the TSO to have all of the necessary security information to direct all travelers to the proper lane, either TSA PreCheck® screening, standard screening, or enhanced screening. The CAT-2 units are

[398] Transportation Safety Administration, "TSA PreCheck: Touchless Identity Solution," (accessed Feb. 7, 2024), https://www.tsa.gov/biometrics-technology/evaluating-facial-identification-technology.
[399] Ibid.
[400] TSA's retention and disposition of facial images for FRT verification are governed by the National Archives and Records Administration (NARA) approved TSA Records Schedule. See DAA-0560-2021-000; available at: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0560/daa-0560-2021-0001_sf115.pdf
[401] Ibid.
[402] Ibid.
[403] Jason Lim, TSA Identity Management Capability Manager, Written Statement for the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, at 2 (hereinafter Lim Statement).

> currently deployed at nearly 60 airports nationwide and will expand to more than 400 federalized airports over the coming years.[404]

Lim's statement additionally explained that CAT-2 screens have clear language notifying travelers of their option to opt out of having their photo taken, and that physical signage at the entrance of the security line checkpoint informs passengers of this option.[405]

U.S. Immigrations and Customs Enforcement (ICE)

Homeland Security Investigations (HSI), the investigative arm of ICE, reported using Clearview AI to support its criminal investigations.[406] In the course of an investigation, HSI may encounter digital images of potential victims or individuals suspected of crimes that HSI cannot connect to identifiable information through other investigative means and methods.[407] HSI then submits these images to government agencies and commercial vendors to compare against their digital image galleries via facial recognition processes. The agencies and vendors query their databases for potential matches and return lists of potential matches that HSI can use to produce investigative leads.[408]

During the period in which GAO inquired as to federal law enforcement utilization of FRT (October 2019 through March 2022), HSI was the only agency that required staff to take FRT training prior to using services.[409] In 2021, HSI implemented two training requirements that staff must complete prior to using Clearview AI.[410]

In 2023, HSI was contacted by law enforcement in the United Kingdom regarding a sexually explicit video that appeared to originate in America.[411] HSI ran the faces through FRT and were able to identify the man, and through additional investigation corroborated the match and arrested him on charges of sexual exploitation of a child.[412] Forbes reported that HSI uses FRT to solve "years-old crimes that's led to hundreds of identifications of children and abusers."[413]

---

[404] Lim Statement, at 2.
[405] Ibid.
[406] U.S. Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties,* Sept. 2023, https://www.gao.gov/products/gao-23-105607.
[407] U.S. Dep't of Homeland Security, *Privacy Impact Assessment for the ICE Use of Facial Recognition Services,* May 13, 2020, https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf.
[408] Ibid.
[409] U.S. Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties,* Sept. 2023, https://www.gao.gov/products/gao-23-105607.
[410] Ibid.
[411] Thomas Brewster, "AI facial recognition used in thousands of child exploitation cold cases," *Forbes*, Aug. 7, 2023, https://www.forbes.com/sites/thomasbrewster/2023/08/07/dhs-ai-facial-recognition-solving-child-exploitation-cold-cases/?sh=4f9d5c0d7682.
[412] Ibid.
[413] Ibid. HSI declined to confirm or comment on the operations' existence, therefore, this quotation may not be attributed to HIS.

Emerging Civil Rights Concerns

The Center for Democracy & Technology reports that current ICE policies permit use of facial recognition technology "'in furtherance of ongoing investigations,' allowing broad use of facial recognition to identify individuals beyond just criminal suspects and individuals believed to have violated immigration law."[414]

A 2022 report from the Georgetown Law Center on Privacy & Technology, *American Dragnet*, found that ICE has used FRT to search through the driver's license photos of one in every three (32 percent) adults in the U.S.[415] Research shows that ICE has been conducting FRT searches since 2008, when it contracted with a biometrics company, L-1 Identity Solutions. This contract allowed ICE to access Rhode Island's department of motor vehicles' face recognition database to "recognize criminal aliens."[416] More recently, researchers have also found that in at least six of the 17 jurisdictions that allow undocumented individuals to apply for driver's licenses, ICE has used FRT to scan drivers' license photographs for deportation purposes.[417]

The report opines that ICE had built a "dragnet surveillance system" by "reaching into the digital records of state and local governments and buying databases with billions of data points from private companies."[418] The report argues that to create its surveillance system, ICE is exploiting people's trust in institutions since ICE can conduct a warrantless search through state driver records for civil immigration enforcement.[419] Alvaro Bedoya, Commissioner at the Federal Trade Commission (FTC) and former Director of Georgetown Law's Center on Privacy and Technology, explained that this is "a huge betrayal of undocumented people… [ICE agents are] taking advantage of that [licensure] to secretly find and deport those people using face recognition technology."[420] However, DHS indicated that Enforcement and Removal Operations does not focus on random people but "prioritizes dangerous noncitizens who undermine public safety."[421]

For asylum seekers arriving at the U.S. border or ports of entry, CBP has implemented the use of the mobile app CBP One, which serves as a single portal to a variety of CBP services, such as advance submission and appointment scheduling.[422] In 2023, it was reported that non-profit organizations assisting Black asylum seekers found that the app was failing to register people with darker skin

---

[414] Center for Democracy & Technology, "Transparency and Policy Recommendations for Federal Law Enforcement Use of Facial Recognition," Jan. 19, 2024, https://cdt.org/wp-content/uploads/2024/01/DOJ-DHS-Comment-Transparency-and-Policy-Recommendations-for-Federal-Law-Enforcement-Use-of-Facial-Recognition.pdf.
[415] Georgetown Law Center on Privacy & Technology, *American Dragnet: Data-Driven Deportation in the 21st Century,* May 10, 2022, https://americandragnet.org/.
[416] Ibid.
[417] Ibid.
[418] Georgetown Law Center on Privacy & Technology, *American Dragnet: Data-Driven Deportation in the 21st Century*, May 10, 2022, https://americandragnet.org/.
[419] Ibid.
[420] Amanda Levendowski, *Resisting Face Surveillance with Copyright Law*, 104 N.C. L. Rev. 1015 (2022) (Introduction, I. A).
[421] DHS Affected Agency Review, Jun. 28, 2024.
[422] U.S. Customs and Border Protection, "CBP One™ Mobile Application," https://www.cbp.gov/about/mobile-apps-directory/cbpone (accessed Mar. 26, 2024).

tones.[423] People from Haiti and African countries, in particular, were finding the app unable to map their features, preventing them from uploading photos in order to receive an asylum appointment.[424]

In 2024, CBP said that biometric traveler verification service matching has a match rate of 99.4 percent on entry and 98.1 percent on exit, and that between 2017 and 2022, people using the system from African countries in had a 99.5 percent match rate, while people coming from Central American countries had a 99.6 percent match rate.[425] As of the writing of this report, DHS's Office of Inspector General is conducting an investigation to assess whether CBP adequately planned to process asylum seekers on the Southwest border with the CBP One app.[426]

GAO reported in 2023 that CBP had not assessed whether staff had appropriate skills and competencies to use commercial facial recognition services.[427] Acting Executive Assistant Commissioner Diane Sabatino testified that web-based training that would serve as baselines training for CBP personnel using any type of FRT has been under development and CBP expects implementation in April 2024.[428] As of June 2024, this recommendation is classified as "Open,"[429] as CBP is in the process of completing corrective actions to address the training need identified by GAO.[430] GAO also made three recommendations to DHS related to training for facial recognition services and two recommendations related to privacy requirements; DHS concurred with the recommendations and said it would develop specific training and guidance on the use of FRT. DHS also said its Privacy Office would continue to work with components using FRT to ensure adherence to privacy requirements.[431] As of February 2024, it had not yet implemented the recommendations, however, some agencies had begun to address outstanding privacy requirements identified in the GAO review.[432]

One concern raised at the Commission's briefing about TSA's utilization of FRT at airport security checkpoints regarded consent. Jason Lim, Identity Management Capability Manager for TSA, testified that U.S. citizens are free to opt out of having their photos taken at TSA security

---

[423] Melissa del Bosque, "Facial recognition bias frustrates Black asylum applicants to US, advocates say," *The Guardian,* Feb. 8, 2023, https://www.theguardian.com/us-news/2023/feb/08/us-immigration-cbp-one-app-facial-recognition-bias.
[424] Ibid.
[425] FedScoop, "CBP leaning into biometrics on controversial app, raising concerns from immigrant rights advocates," Mar. 7, 2024, https://fedscoop.com/cbp-one-app-biometrics-immigrants-rights/.
[426] DHS Office of Inspector General, "Ongoing Projects," https://www.oig.dhs.gov/reports/ongoing-projects (accessed May 22, 2024).
[427] U.S. Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties,* Sept. 2023, https://www.gao.gov/products/gao-23-105607.
[428] Acting Executive Assistant Commissioner Diane Sabatino, CBP Office of Field Operations, testimony, *Facial Recognition Technology Briefing*, p. 120.
[429] U.S. Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties,* Sept. 2023, https://www.gao.gov/products/gao-23-105607.
[430] U.S. Dep't of Homeland Security, DHS Responses to U.S. Commission on Civil Rights Interrogatories, Apr. 17, 2024, at 17.
[431] Goodwin Statement, at 9.
[432] Ibid., at 8-9.

checkpoints, and passengers were notified of this right via postage signage that is available in English and Spanish.[433]

Lim testified:

> [Y]ou can always opt out of facial recognition by declining to have your photo taken. This will not impact your place in the line or cause undue delays in your screening process. And when you opt out, our offices will literally turn off the camera to ensure that your photo is not even accidentally captured. And we have posted physical signs along the queue and near our devices to inform the passengers of their right to opt out. And additionally, we have integrated this opt out language into the passenger-facing user interface screen itself so that we want to maximize the opportunity for passengers to know that they have the option to decline the photo.[434]

During the Commission's briefing, questions were raised about whether such signage is prominently displayed, whether passengers actually know that they have this right, and, if they do, whether they feel empowered to invoke it.[435] Laura MacCleery, Senior Director of Policy at UnidosUS, explained:

> Why don't we opt out when we approach that checkpoint? Well, it's about the power dynamics of withholding our consent. We're approaching an official checkpoint that has the power to disrupt our plans on a ticket we've already bought, and most people would not be [] well informed [] that they can opt out without penalty or consequence. They would simply defer. So, this question of power dynamics and how technology shows up in the real world, who knows how it works and who doesn't? . . . We have to think about the real-world testing and the power dynamics that are implicit in any of these situations in order to understand the civil rights implications.[436]

This echoes information elicited by the Algorithmic Justice League's initiative gathering information from individuals traveling through airports: preliminary data indicates over 85 percent of respondents stated there was a lack of signage making it clear that opting out was an option, and over 95 percent of respondents indicated that TSA agents did not ask for their participation to be scanned.[437] According to DHS, between January 1, 2018 and February 28, 2024, 247,338 individuals opted out of biometric scanning by CBP at entry (approximately .05 percent of all encounters).[438]

---

[433] *See, supra* note 405.
[434] Jason Lim, Identity Management Capability Manager, Transportation Security Administration, testimony, *Facial Recognition Technology Briefing*, p. 106.
[435] *Facial Recognition Technology Briefing* transcript, pp. 118-120.
[436] Laura MacCleery, Senior Director of Policy, UnidosUS, testimony, *Facial Recognition Technology Briefing*, pp. 149-150.
[437] Buolamwini Statement, at 5-6.
[438] U.S. Dep't of Homeland Security, DHS Response to U.S. Commission on Civil Rights Interrogatories, Apr. 17, 2024.

Agency Efforts

DHS indicated to the Commission that according to the DHS AI Roadmap, in line with the DHS's commitment to transparency and visibility into the Department's vision for AI and to ensuring responsible use, DHS will continue to publicly share information about its own activities and use.[439] The DHS AI Use Case Inventory[440] is a practice to ensure the Department is sharing the technical advances of AI with other Federal agencies as well as with academia and the public.[441]

In 2023, DHS Chief Information Officer Eric Hysen testified before the House Subcommittee on Cybersecurity, Information Technology, and Government Innovation regarding federal use of artificial intelligence. Hysen indicated that "DHS will lead in the responsible use of AI to secure the homeland and defend against malicious use of this transformational technology. As we do this, we will ensure that our use of AI fully respects civil and human rights, is rigorously tested to avoid bias, disparate impact, privacy harms, and other risks, and that it is clearly explainable to the people we serve."[442] DHS assigned Hysen and the Under Secretary for Science and Technology to chair a Department-wide AI task force.[443]

In August 2023, Secretary Mayorkas signed DHS Policy Statement 139-06, "Acquisition and Use of Artificial Intelligence and Machine Learning Technologies by DHS Components." It indicates that DHS will not collect, use, or disseminate data used in AI activities, or establish AI-enabled systems that make or support decisions, based on the inappropriate consideration of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, age, nationality, medical condition, or disability, and that DHS will continually strive to minimize inappropriate bias utilizing standards required by law and policy.[444] The policy continues to state that:

> DHS, with external assistance where appropriate, will test and validate AI employed in use cases where discriminatory activity or effects may be possible, to ensure impermissible discrimination is not occurring and to aid in advancing equity and fundamentally fair treatment. DHS will also use civil rights evaluation methods, including disparate impact analysis where appropriate, to detect impermissible discriminatory treatment that may result from the use of AI in DHS processes and activities. The threshold civil rights and civil

[439] DHS Affected Agency Review, Jun. 28, 2024.
[440] U.S. Dep't of Homeland Security, "Artificial Intelligence Use Case Inventory," https://www.dhs.gov/data/AI_inventory (accessed Jul. 2, 2024).
[441] DHS Affected Agency Review, Jun. 28, 2024.
[442] Eric Hysen, Chief Information Officer, Dep't of Homeland Security, Testimony before the Subcommittee on Cybersecurity, Information Technology, and Government Innovation of the House Committee on Oversight and Accountability on "How are Federal Agencies Harnessing Artificial Intelligence?" Sept. 14, 2023, https://oversight.house.gov/hearing/how-are-federal-agencies-harnessing-artificial-intelligence/.
[443] Ibid.
[444] U.S. Dep't of Homeland Security, "Acquisition and Use of Artificial Intelligence and Machine Learning Technologies by DHS Components," Aug. 8, 2023, https://www.dhs.gov/sites/default/files/2023-09/23_0913_mgmt_139-06-acquistion-use-ai-technologies-dhs-components.pdf.

> liberties compliance question for AI is whether the algorithm complies with the applicable law and policy governing the domain in which the AI is implemented.[445]

In September 2023, DHS issued a Department-wide directive establishing the authorized use of facial recognition and face capture throughout DHS.[446] The scope of the directive applies to all facial recognition and face capture technologies used "including technologies used by Federal, State, Local, Tribal and Territorial government, non-U.S. government, and international entities operated by or on behalf of the Department."[447] The directive, among other things, requires that DHS and its subcomponents "develop accuracy and performance metrics, and procedures for testing and evaluating [facial recognition] and [facial capture] technologies in accordance with International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standards and technical guidance issued by National Institute of Standards and Technology (NIST)."[448] The directive also requires the Department to endeavor to "minimize[e] bias in operational use, and safeguard[] individuals against disparate impacts based on protected characteristics."[449] The directive further states that "DHS…does not collect, use, disseminate, or retain [facial recognition] or [facial capture] information solely based on race, ethnicity, national origin, religion, gender, gender identity, age, sexual orientation, medical condition, or disability."[450] The directive does not apply to research and development and does not replace civil rights and civil liberties regulations and safeguards with respect to FRT.[451]

Peter Mina of DHS's CRCL indicated in his written statement to the Commission that CRCL considers several broad themes when reviewing and supporting DHS's FRT programs, including discrimination, accuracy, scale, flexibility, use, perception, redress, unintended consequences, and validation.[452] Regarding validation, Mina wrote:

> Analysis of accuracy and error rates need to account for the various factors potentially presented in an operational setting, such as an airport. Objective, independent analysis of software and algorithms ensures that the system is operating as we believe it is, and verifies that the Department's biometric data remains secure and that technical protections are effective and implemented properly.[453]

Mina explained that some of the key parts of the directive:

---

[445] Ibid.
[446] Use of Face Recognition and Face Capture Technologies, DHS Directive, Directive No. 026-11, Sept. 11, 2023, https://www.dhs.gov/sites/default/files/2023-09/23_0913_mgmt_026-11-use-face-recognition-face-capture-technologies.pdf
[447] Ibid., Sect. II.
[448] Ibid., Section IV, C.
[449] Ibid., Sect. IV, C; IV, F.
[450] Ibid., Sect. V. A.3.
[451] Ibid., Sect. II. For a full list of the DHS Management Directives on Information and Technology Management see https://www.dhs.gov/publication/information-and-technology-management
[452] Mina Statement, at 4.
[453] Ibid.

- Dictate that all uses of facial recognition and face capture technologies be "thoroughly tested to ensure that there is no unintended bias or disparate impact in accordance with national standards."
- Direct a review of all existing uses of FRT and conduct periodic testing and evaluation to ensure that the systems meet performance goals.
- Require that U.S. citizens be afforded the right to opt out of FRT for specific non-law enforcement uses.
- Prohibit FRT from being the sole basis for any law or civil enforcement-related action.
- Establish a process for Department oversight offices, including the Privacy Office, CRCL, the Science and Technology Directorate, and the Office of the Chief Information Officer to review all new uses of face recognition and face capture technologies before they are implemented.[454]

DHS asserts that this directive ensures the technology is implemented and deployed responsibly and that the Department is "proactively assessing" its utilization.[455]

DHS indicated that it has reviewed all existing uses of the Department's use of face recognition and face capture technology and is continuing its work with other DHS components and programs on these and any newly identified use cases to ensure programs and activities include robust civil rights and civil liberties protections.[456]

In May 2024, DHS also released their "Innovation, Research & Development Strategic Plan" for the fiscal years 2024 through 2030.[457] Included in the report are various DHS "Missions" in which Innovation, Research & Development drives technological advancement. The report also includes Strategic Priority Research Areas (SPRA) to address needs across those mission areas. The report highlights emerging technology as a priority for DHS. While the term "facial recognition" is only specifically mentioned once, the report includes an "Artificial Intelligence and Autonomous Systems" section that outlines future capabilities suggesting the use of FRT-like technology such as automated "threat detection to safely screen people," "digital media exploitation," "detection of immigration fraud," and "biometric and identity verification capabilities."[458] The "Digital Identity and Trust" SPRA notes that "Digital Identity is used to verify the identity of entities (natural person, non-person). The ability to establish and verify an individual's identity using asserted identity and biometric information enables the Department to perform risk-based decision making that is tailored to the individual."[459]

---

[454] Mina Testimony, pp. 87-88.
[455] Ibid.
[456] DHS Affected Agency Review, Jun. 28, 2024.
[457] U.S. Dep't of Homeland Security, *DHS Innovation, Research & Development Strategic Plan, Fiscal Years 2024-2030,* https://www.dhs.gov/sites/default/files/2024-05/24_0513_dhs_ird_strategic_plan_fy24-30_0.pdf.
[458] Ibid.
[459] Ibid. U.S. Citizenship and Immigration Services (USCIS) Fraud Detection and National Security Directorate (FDNS) officers with approved access to the FR system within Consular Consolidated Database may utilize this feature, however as of June 28, 2024, FDNS does not track USCIS use of external agency-owned FRT and cannot provide metrics on false positives. DHS Affected Agency Review, Jun. 28, 2024.

Testing FRT: DHS Maryland Test Facility

DHS S&T funds FRT research, testing, and evaluation with grant funding from the National Science Foundation. The funding covers S&T's Maryland Test Facility (MdTF), a 24,000 square foot laboratory space fully instrumented and designed for scenario testing of biometric systems using human subject testing.[460] MdTF opened in 2014 to support S&T and CBP's Apex Air Entry/Exit Re-engineering (AEER) project.[461] The AEER project created a partnership between S&T and CBP to test and evaluate operational processes using biometric and non-biometric technologies in order to increase security while facilitating trade and travel, and implement capabilities required by federal legislation.[462] MdTF is operated by the Science Applications International Corporation's (SAIC) Identity and Data Sciences Laboratory (IDSL). SAIC is a government contractor specializing in technology integrations,[463] and IDSL was founded in 2010 to support US Government initiatives by providing biometric and identity research, development, testing, and evaluation (RDT&E).[464] Through MdTF, IDSL has evaluated hundreds of face, finger, and iris systems to gather biometric performance and demographic variation metrics.[465]

On April 18, 2024, a bipartisan committee consisting of several Commissioners and Commission staff toured MdTF, where DHS staff provided an overview of the vision of MdTF as well as the types of FRT testing conducted at the lab. DHS staff explained that the MdTF advances DHS's Biometric & Identity Technology Center's vision of 1) driving biometric and identity innovation, 2) facilitating and accelerating understanding of biometrics and identity technologies for new use cases, and 3) following a "build once, use widely" approach through holding yearly "Rallies" focused on several use cases and commercial facial recognition technologies.[466] The goals guiding MdTF's operation include 1) driving efficiencies by supporting cross cutting methods and best practices, 2) delivering subject matter expertise across the DHS enterprise, 3) engaging the industry and providing feedback, and 4) encouraging innovation with industry and academia.[467]

MdTF is fully instrumented and designed for human subject testing, so the types of FRT testing conducted include, but go beyond, the type of algorithmic testing that NIST focuses on. The three types of MdTF testing include:

- Technology testing, which assesses the algorithms and whether they function as intended;
- Scenario testing, which focuses on use-cases and gathers biometric samples to assess the full biometric system. This testing is intended to mimic an operational application of technology

[460] Vemury Statement, at 1.
[461] The Maryland Test Facility, https://mdtf.org/.
[462] U.S. Dep't of Homeland Security, Science & Technology Directorate, "Apex AEER Program," https://www.dhs.gov/science-and-technology/apex-aeer (accessed Jun. 28, 2024).
[463] SAIC, "About SAC," https://www.saic.com/who-we-are/about-saic (accessed Jun. 28, 2024).
[464] U.S. Dep't of Homeland Security, Science & Technology Directorate, Site Visit Presentation at MdTF, Apr. 18, 2024.
[465] Ibid.
[466] Ibid.
[467] Ibid.

while simultaneously instituting controls on the procedure, essentially predicting how that system would operate in the real world;[468] and

- Operational testing, which tests a technology in its actual location (such as a deployed FRT system in an airport), measuring the user-system interaction effects.[469]

These three types of testing represent different steps in the FRT testing process and are distinct from the NIST testing discussed previously. NIST testing focuses on technology testing, which is the testing of the algorithm itself. Results from NIST tests can establish performance measures for a particular algorithm, which can then be compared to other algorithms.[470] A benefit of this type of testing is that it provides insights on how the technology is developing over time. Vendors often cite their accuracy ratings based upon this type of testing. For example, Clearview AI, which is used by some federal agencies and police forces, highlights their 99 percentile accuracy results from NIST as an example of their algorithm's accuracy capabilities.[471] While this testing is important, when used alone, it cannot accurately determine how an algorithm will work if deployed in a real-world context while interacting with human users.

As discussed earlier in this report, a top performing algorithm alone does not guarantee accuracy, so tests performed at MdTF assess the technology using scenario testing. MdTF accomplishes this by simulating full facial recognition systems that individuals in the real-world may interact with, such as going through airport security or applying for a visa. These tests are conducted using volunteers who, under informed consent, sign up to act as users of the technology. The tests are performed to meet DHS's operational needs, for example, developing more accurate and easier security screening for TSA and CBP.[472]

The MdTF testing volunteers are integral to the success of scenario testing, and MdTF focuses on recruiting volunteers with diverse demographics through an ethical data collection approach consistent with Institutional Review Board (IRB) standards.[473] MdTF volunteers provide informed consent and agree to provide data for MdTF's purposes.[474] MdTF volunteers range in age from 18 to 84, include a multitude of races and ethnicities, span the gender spectrum, and represent a wide

[468] National Institute pf Standards and Technology, "Scenario Test," https://csrc.nist.gov/glossary/term/scenario_test (accessed Jun. 28, 2024).
[469] National Institute pf Standards and Technology, "Operational Test," https://csrc.nist.gov/glossary/term/operational_test (accessed Jun. 28, 2024).
[470] *See, supra* notes 158-163.
[471] Ton-That Statement, at 1.
[472] Vemury Statement, at 2.
[473] An IRB is an objective third party tasked with protecting and managing risk to human research subjects; all research projects involving human subjects should be reviewed by an IRB. U.S. Dep't of Homeland Security, *Institutional Review Board Frequently Asked Questions for TVTP Grantees and Applicants,* Sep. 27, 2023, https://www.dhs.gov/sites/default/files/2024-03/23_0927_cp3_irb-faqs-for-tvtp.pdf.
[474] MdTF Informed Consent, rec'd at U.S. Dep't of Homeland Security, Science & Technology Directorate, Site Visit Presentation at MdTF, Apr. 18, 2024.

distribution of measured skin tones.[475] As of November 2023, there have been 3,657 unique volunteers from 102 countries of origin supporting MdTF's research.[476]

MdTF executes its scenario testing through simulated events called Biometric Technology Rallies. These Rallies are yearly biometric system evaluations focused on commercial systems deployed in DHS technology use-cases. During a Rally, MdTF has a diverse set of volunteers move through several phases of a biometric capture simulation, for example, travelers going through TSA facial screening. While the biometric system captures the volunteers' data and images, MdTF is controlling for several different commercial solutions for both acquisition (i.e., image capture through a camera) and matching (i.e., algorithms used to match the captured image to the correct volunteer). An example of a Rally can be broken down into six phases:

- Informed Consent: participants are briefed about the Rally and consent to participate
- Ground Truth Data Gathering: volunteers self-report their gender and race, and staff measure their skin tone using specialized colorimeters.
- Camera Acquisition Without Masks: an acquisition camera system takes a photo of each person without a mask
- Camera Acquisition With Masks: an acquisition camera system takes a photo of each person with a mask
- Algorithm Matching: matching systems find the face in each photo and compare it to known people to identify the person in the photo
- Reporting: performance is measured for various possible combinations of acquisition and matching systems

The completion of a Rally provides comprehensive metrics about the tested systems' efficiency, effectiveness, satisfaction, and equitability for given use cases. For example, MdTF's 2021 Rally focused on testing the ability of commercial biometric systems to reliably acquire and match images of diverse individuals, including those wearing face masks.[477] The tests assessed how accurate the photo acquisition system (i.e., camera) worked with a corresponding matching system (i.e., accuracy of properly identifying and matching faces) and compared those systems' performance across skin tones, race, and gender groups.[478] Essentially, volunteers had their image captured by camera both with and without a mask, and those images were sent to matching systems to identify the person in the photo.[479] This assessment allowed MdTF to test performance for each of fifty possible combinations of acquisition and matching systems, measuring against a common accuracy benchmark of 95 percent.[480]

---

[475] U.S. Dep't of Homeland Security, Science & Technology Directorate, Site Visit Presentation at MdTF, Apr. 18, 2024.
[476] Ibid.
[477] Ibid.
[478] MdTF, "2021 Biometric Technology Rally," https://mdtf.org/Rally2021#:~:text=The%202021%20Biometric%20Technology%20Rally%20will%20demonstrate%20the%20ability%20of,including%20those%20wearing%20face%20masks.
[479] Ibid.
[480] Ibid.

MdTF's 2022 Rally focused on processing groups of people traveling together with the goal of challenging the industry to develop faster, more accurate, and easier-to-use biometric recognition capabilities to improve security and ease of use at security checkpoints.[481] Volunteers formed groups of two and four, and walked through a simulated security checkpoint where the acquisition systems had to select the best photo from each volunteer in the group to submit for matching.[482] Then, the matching systems attempted to identify the face in each photo by comparing it to photos of known people.[483] MdTF found that one of the largest sources of error in FRT results is when a system "fails to acquire" an image.[484] Put differently, this can occur when the system cannot effectively acquire or process an image in a given time period,[485] therefore suggesting that the failure may be with the image acquisition system, and not the algorithm.[486] As a result from their 2022 Rally, MdTF explained that "without significant modernization of capture procedures, recognition errors will become more prevalent as volumes [of people] increase."[487] Since 2018, MdTF has tested more than 200 combinations of commercial facial acquisition systems and matching algorithms, exemplifying their "build once, use widely" approach.[488]

A benefit of scenario testing is that it can provide insight into how an FRT system (i.e., the combination of the algorithm and camera) may work if deployed in the field at lower cost than operational testing. Another benefit to scenario testing is that it allows vendors to test their systems prior to it being used in the real world, where failed systems can not only be costly but also result in civil rights concerns if a system has high false positive and/or false negative results. Additionally, since scenario testing is conducted in a controlled laboratory setting, researchers can control each stage of the experiment. Scenario testing can isolate which parts of the system (e.g., the algorithm, camera lens, camera resolution, camera placement, etc.) are accurate and which parts need adjustment. These adjustments are possible in a laboratory setting, unlike in the real world, where there are multiple variables at play that may not be controllable. This allows DHS to utilize scenario testing and the results from the MdTF prior to an FRT system being tested in the real world (i.e., operational testing).[489] The downside to this type of scenario testing is that it is resource intensive and can only be conducted several times a year (but can be scaled up with additional resources).

As this report has discussed, a main concern regarding FRT is the match differentials (both false positives and false negatives) for different demographic groups. To address this, researchers at MdTF

---

[481] MdTF, "The 2022 Biometric Technology Rally," https://mdtf.org/Rally2022.
[482] S&T Directorate MdTF Presentation
[483] Ibid.
[484] Failure to Acquire is an effectiveness measurement representing the percentage of image capture transactions that result in a failure to acquire or process image captures within a given time interval; it has to do with acquisition systems, not matching algorithms. *See* MdTF, "Rally Metrics," https://mdtf.org/Rally/Metrics
[485] U.S. Dep't of Homeland Security, Science & Technology Directorate, Site Visit Presentation at MdTF, Apr. 18, 2024.
[486] MdTF, "Rally Metrics," https://mdtf.org/Rally/Metrics.
[487] U.S. Dep't of Homeland Security, Science & Technology Directorate, Site Visit Presentation at MdTF, Apr. 18, 2024; *see also*, International Organization for Standardization and the International Electrotechnical Commission, Draft International Standard 29794-5: 2023, https://www.iso.org/standard/81005.html.
[488] U.S. Dep't of Homeland Security, Science & Technology Directorate, Site Visit Presentation at MdTF, Apr. 18, 2024.
[489] Ibid.

collect volunteers' demographic data to test whether the FRT correctly captures the intended information, such as its ability to accurately capture an individual's skin tone. FRT is available on many types of devices, and the technology's performance varies depending on how well different cameras capture an individual's physical characteristics. While many critiques about FRT focus on the algorithms and their accuracy rates, researchers at MdTF explained that most errors that occur in scenario testing are not due to algorithms, but rather camera quality.[490] During the Commission's site visit, participants saw an example of twelve different images of one volunteer on the same day and under consistent lighting taken from different cameras. Different cameras resulting in one person being captured with a wide range of skin tones highlights the importance of understanding the limitations of FRT when applied with inadequate camera technology.

Arun Vemury of DHS S&T testified that through scenario testing, DHS has found that camera technologies can either fail to capture images, or capture lower quality images, for people with darker skin tones. To mitigate these risks, Vemury stated that DHS plans to leverage skin tone measurements made from real people during scenario testing to create a standard reference material for human skin to calibrate and assess face capture systems.[491] Vemury noted during the Commission's tour, that as technology continues to develop, the best-performing systems (i.e., the ones combining high-performing algorithms and cameras) will theoretically perform well across all demographic groups.[492] However, DHS recognizes that an FRT match may cognitively bias a reviewer's judgment of face similarity and reduce the likelihood of detecting a false positive.[493] Early research suggests that reviewers may also be more likely to trust the technology and accept the result, regardless of its validity.[494] In forensic feature-comparison disciplines, cognitive bias is such that humans may tend to naturally focus on similarities between samples and discount differences.[495] DHS indicated that because these errors are more likely to occur when the image quality is low, S&T developed a framework for "human-algorithm teaming" (explained below) to ensure that the performance of the full system—including human operators—can be measured and optimized.[496]

In response to follow-up questions from the Commission's site visit, S&T indicated that scenario testing is important when certain changes in technology or processes have taken place in a facial recognition system. These changes include developments in technologies used in collecting face imagery, changes in collection processes or environmental conditions, expansion of subject population beyond the scope of previous eligibility (e.g., if a system was previously evaluated with people from age 18-65, but subsequently expanded to ages 12-95), or as frequently as determined by

[490] Ibid.
[491] Vemury Statement, at 2.
[492] U.S. Dep't of Homeland Security, Science & Technology Directorate, Site Visit Presentation at MdTF, Apr. 18, 2024.
[493] Vemury Statement, at 2-3
[494] *See, supra* note 177.
[495] Executive Office of the President, *Report to the President: Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods,* Sept. 2016, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf.
[496] Vemury Statement, at 3.

law and policy.[497] S&T noted that the current DHS Directive 026-11 requires testing no less than every three years.

S&T also expanded on how they conceived the proper roles and responsibilities for different entities taking part in an FRT system. Suggestions included:

- Developers: responsible for laboratory testing with relevant benchmark data (e.g. submitting free or licensed software to NIST testing, etc.)
- System Owners & Integrators: responsible for scenario testing of capabilities to verify performance with relevant data and simulated operational conditions
- System Owners & Deployers: responsible for operational testing of capabilities to verify performance with relevant data and operational conditions
- Federal Agencies: responsible for creating sequestered benchmark datasets for testing and validating performance testing based on appropriate standards, policies, and laws, as well as setting testing requirements
- Testing Laboratories: responsible for curating and maintaining sequestered ethically collected datasets, designing and executing standards-compliant tests that meet government testing requirements for biometric systems, and reporting results.

Along with their yearly Rallies, MdTF publishes several peer-reviewed scientific studies. As this report has explained, the AI used in FRT is just one component of an overall system of the monitoring, surveilling, and analyzing enabled by FRT. Other targeted studies that MdTF has run have focused on specific processes, results, or frameworks that illustrate other patterns worth considering when engineering effective and equitable FRT systems.[498]

One such process within an FRT system is known as "human algorithm teaming" which is when humans review algorithmic results to make an identity determination. In one 2020 study conducted by the MdTF team, the researchers explored how algorithmic outcomes may cognitively bias the human decision making process.[499] The Commission heard many experts testify about the concern that human reviewers of FRT results are not an effective backstop to accuracy.[500] MdTF's study found that "face recognition algorithms incorporated into a human process can influence human responses, likely limiting the total system performance" and acknowledged that much additional research is needed in this relatively new field.[501] Another MdTF study found that when study participants were wearing masks, this increased the likelihood of automation bias and the human

[497] U.S. Dep't of Homeland Security, Science & Technology Directorate, Follow-Up Responses to MdTF Site Visit.
[498] U.S. Dep't of Homeland Security, Science & Technology Directorate, Site Visit Presentation at MdTF, Apr. 18, 2024.
[499] Howard JJ, Rabbitt LR, Sirotin YB (2020) Human-algorithm teaming in face recognition: How algorithm outcomes cognitively bias human decision-making. PLoS ONE 15(8): e0237855. https://doi.org/10.1371/journal.pone.0237855
[500] Georgetown Law Center on Privacy & Technology, *The Perpetual Line-Up: Unregulated Police Face Recognition in America,* Oct. 18, 2016, https://www.perpetuallineup.org/.
[501] Howard JJ, Rabbitt LR, Sirotin YB (2020) Human-algorithm teaming in face recognition: How algorithm outcomes cognitively bias human decision-making. PLoS ONE 15(8): e0237855. https://doi.org/10.1371/journal.pone.0237855

reviewer's reliance on the algorithm's results to match unfamiliar faces,[502] a scenario where humans are already generally poor at matching.[503]

The MdTF team explained to the Commission that they also leverage their research to review and envision solutions and frameworks for AI-enabled biometric systems. For instance, in a 2023 study, researchers explored the appropriate allocation of tasks between humans and algorithms to improve the overall performance of biometric systems. The study highlighted the importance of considering human-algorithm teams as technology continues to advancement. The study also highlighted that, while biometric research has largely focused on forensic scenarios, there is a need to address use cases which involve a large portion of the population (e.g., airport security checkpoints).

While scenario testing is a necessary step beyond just technology testing, MdTF researchers explained that it is still not sufficient for real-world applications. Fully determining how a particular FRT system operates can only be accomplished through operational testing. For example, testing how a facial recognition system works when it is utilized in an airport. An operational test, like a scenario test, would test the full biometric system. Unlike scenario testing, operational testing works with a larger sample size (e.g., the actual population of subjects passing through an airport) and has less control over how the study is conducted. Furthermore, operational testing has less verifiable ground-truth information, especially regarding self-reported demographics.[504] To support operational testing needs, results of research and testing done by S&T are shared across DHS offices to communicate about the performance of technologies available for purchase. This helps offices understand how to specify relevant metrics and performance benchmarks for their procurements.[505] DHS is also working toward the development of a new international standard to address methods of evaluating biometric systems for demographic effects on performance and plans to add other standardization efforts relevant to face recognition, such as how to handle different levels of facial image quality.[506]

The Commission's visit to MdTF was a unique effort to gain a critical understanding in the importance of testing before the deployment of FRT. As federal agencies that are legally bound to protect civil and constitutional rights, understanding the technology's implications allows the government to prioritize meaningful oversight that supports innovation while protecting those rights.

[502] Barragan D, Howard JJ, Rabbitt LR, Sirotin YB. COVID-19 masks increase the influence of face recognition algorithm decisions on human decisions in unfamiliar face matching. PLoS One. 2022 Nov 21;17(11):e0277625. doi: 10.1371/journal.pone.0277625. PMID: 36409731; PMCID: PMC9678274.
[503] Howard JJ, Rabbitt LR, Sirotin YB (2020) Human-algorithm teaming in face recognition: How algorithm outcomes cognitively bias human decision-making. PLoS ONE 15(8): e0237855.
[504] U.S. Dep't of Homeland Security, Science & Technology Directorate, Site Visit Presentation at MdTF, Apr. 18, 2024.
[505] Vemury Statement, at 3.
[506] Ibid.

U.S. Department of Housing and Urban Development (HUD)

Congress established the U.S. Department of Housing and Urban Development in 1965.[507] As of the writing of this report, Acting Secretary Adrianne Todman is leading HUD, following the resignation of Secretary Marcia Fudge on March 11, 2024.[508]

HUD states on its website that its mission is to

> create strong, sustainable, inclusive communities and quality affordable homes for all. HUD is working to strengthen the housing market to bolster the economy and protect consumers; meet the need for quality affordable rental homes; utilize housing as a platform for improving quality of life; build inclusive and sustainable communities free from discrimination, and transform the way HUD does business.[509]

HUD reports that it strives to uphold its mission by administering federal programs and creating housing policy that can help create affordable housing opportunities in the rental and sales markets for individuals and families; combat homelessness; promote fair housing and inclusive community development; and foster sustainability.[510]

HUD's Office of Fair Housing and Equal Opportunity (FHEO) is the primary office that handles external civil rights enforcement, in conjunction with the Office of the General Counsel (OGC). The mission of FHEO is to "eliminate housing discrimination, promote economic opportunity, and achieve diverse, inclusive communities by leading the nation in the enforcement, administration, development, and public understanding of federal fair housing policies and laws."[511] Through FHEO and OGC, HUD enforces a number of statutes, executive orders, and regulations.[512]

HUD is also responsible for enforcing the Fair Housing Act and other laws that protect people from housing discrimination on the basis of race, color, religion, national origin, sex, disability, and familial status (among other categories).[513] HUD reported to the Commission that it ensures housing providers and grantees comply with other civil rights statutes, executive orders, and regulations.[514] HUD also works to enforce the Fair Housing Act through two programs—the Fair Housing

---

[507] 42 U.S.C. § 3532 (1965).
[508] U.S. Department of Housing and Urban Development, "Statement from HUD Secretary Marcia L. Fudge," Mar. 11, 2024, https://www.hud.gov/press/press_releases_media_advisories/hud_no_24_048.
[509] U.S. Department of Housing and Urban Development, "Mission," https://www.hud.gov/about/mission.
[510] *See generally* U.S. Department of Housing and Urban Development, "Fiscal Year 2022-2026 Strategic Plan," Mar. 28, 2022, https://www.hud.gov/sites/dfiles/CFO/documents/FY2022-2026HUDStrategicPlan.pdf.
[511] U.S. Department of Housing and Urban Development, "Fair Housing and Equal Opportunity," https://www.hud.gov/fairhousing.
[512] *See* U.S. Commission on Civil Rights, *Are Rights A Reality? Evaluating Federal Civil Rights Enforcement*, November 2019, pp.226-27, https://www.usccr.gov/files/pubs/2019/11-21-Are-Rights-a-Reality.pdf.
[513] 42 U.S.C. 3535(d); 42 U.S.C. §§ 3601-19 and implementing regulations at 24 C.F.R. parts 100, 103, and 180; U.S. Dep't of Hous. and Urban Dev., "Fair Housing Rights and Obligations," https://www.hud.gov/program_offices/fair_housing_equal_opp/fair_housing_rights_and_obligations.
[514] *See* U.S. Commission on Civil Rights, *Are Rights A Reality? Evaluating Federal Civil Rights Enforcement*, November 2019, p.227

Assistance Program (FHAP) and the Fair Housing Initiatives Program (FHIP)—which promote fair housing at the state and local levels.[515]

One of the central offices to fulfill HUD's mission is Public and Indian Housing (PIH). This office is responsible for HUD's Housing Choice Voucher, Public Housing, and Native American programs.[516] Within PIH, the office administers several public housing programs such as the Capital Fund, which provides financial assistance to public housing agencies to make improvements to existing public housing.[517] The Capital Fund program provides annual funds to approximately 2,756 public housing agencies (PHAs) across the country.[518] These PHAs may then use these grants for "development, financing, modernization, and management improvements."[519] Although HUD lacks specific rules related to the use of FRT or other AI, HUD's Capital Fund program regulations require all housing authorities receiving grant funds to comply with Title VI of the Civil Rights Act of 1964[520] and HUD's Title VI regulations.[521] HUD's Title VI regulations prohibit HUD grant recipients from using funds in a manner that would have the effect of subjecting persons to discrimination because of their race, color, or national origin.[522]

FRT Utilization

As a component of the Commission's investigation, on February 12, 2024, the Office of Civil Rights Evaluation and the Office of General Counsel sent interrogatories and document requests to HUD to better understand how it utilizes and regulates FRT and other AI in public housing. In response, HUD stated:

> [HUD] does not utilize and has not developed any Facial Recognition Technology (FRT). While HUD has no regulations explicitly governing the use of FRT by program participants, HUD requires program participants to use all funds in accordance with Federal, state, and local laws as well as HUD guidelines and regulations.
>
> HUD does not require specific policies on FRT for Public Housing Authorities (PHA) and does not keep a list of PHAs that elect to use FRT. HUD's funds provide program participants

[515] 42 U.S.C. §§ 3535(d), 3610(f), 3616; 24 C.F.R. parts 115 and 125; U.S. Dep't of Hous. and Urban Dev., "Fair Housing Assistance Program (FHAP)," https://www.hud.gov/program_offices/fair_housing_equal_opp/partners/FHAP; U.S. Dep't of Hous. and Urban Dev., "Fair Housing Initiatives Program," https://www.hud.gov/program_offices/fair_housing_equal_opp/partners/FHIP
[516] U.S. Department of Housing and Urban Development, "Public and Indian Housing," https://www.hud.gov/program_offices/public_indian_housing.
[517] *See* 24 CFR § 905.100.
[518] HUD Affected Agency Review, Jun. 24, 2024.
[519] U.S. Department of Housing and Urban Development, "Office of Capital Improvements – Office of Public Housing Investments," Feb. 25, 2019, https://www.hud.gov/program_offices/public_indian_housing/programs/ph/capfund/aboutus.
[520] 42 U.S.C. 2000d-2000d-4.
[521] *See* 24 CFR Part 1.
[522] 42 U.S.C. §2000d-1; U.S. Dept. of Justice, *Title VI Legal Manual*, Section VII, Proving Discrimination-Disparate Impact, p. 3, https://www.justice.gov/d9/books/attachments/2021/02/03/titlevi_legal_manual_rev._ed.pdf (Agency Title VI Disparate Impact Regulations).

> the flexibility to purchase solutions and make investments that will provide decent, safe, and sanitary housing for residents.[523]

Although HUD itself does not develop or use FRT, PHA grantees can choose to purchase surveillance cameras that utilize FRT.[524] According to a 2023 *Washington Post* investigation, the purchase of these cameras has been facilitated by HUD through its Emergency Safety and Security Grant (ESSG) funding.[525] However, as of April 2023, ESSG funding can no longer be used to purchase FRT.[526]

According to HUD officials, housing agencies have purchased surveillance cameras with the goal of making communities safer,[527] but because HUD does not track the purchase of FRT by its grantees, it is possible that residents' rights in subsidized housing have been infringed.[528] However, without hard data, it is difficult to determine how widespread this issue might be. Data from the 2023 *Washington Post* investigation consisting of interviews with residents and legal aid attorneys, along with court records and correspondence with administrators at more than 60 public housing agencies receiving HUD crime-fighting grants, all show that these cameras are being used to punish residents and catch them in minor violations that jeopardize their lease agreements (e.g., smoking in the wrong area or removing a laundry basket from the communal laundry room) and can result in their evictions.[529] Attorneys who defend tenants in eviction cases also report seeing an uptick in cases that reference surveillance footage as evidence.[530]

At the Commission's briefing, Professor Michelle Ewert, Director of the Washburn Law Clinic at Washburn University School of Law, explained that PHAs are increasingly purchasing FRT to surveil tenants and provide building access in lieu of keys or fobs.[531] Ewert stated:

> PHAs and other affordable housing providers often cite public safety as the reason for the use of this technology. They allege that FRT is safer for building access because keys or fobs

---

[523] U.S. Dep't of Housing and Urban Development, Response to USCCR Interrogatories.
[524] *See e.g.*, HUD Statement, at 1; Ewert Statement, at 1; Douglas MacMillian, "Eyes on the poor: Cameras, facial recognition watch over public housing," *The Washington Post*, May 16, 2023, https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/; Lisa Desjardins and Andrew Corkery, "How surveillance camera are being used to punish public housing residents," PBS News, June 4, 2023, https://www.pbs.org/newshour/show/how-surveillance-cameras-are-being-used-to-punish-public-housing-residents; Rep. Maxine Waters and Rep. Ayanna Pressley, Letter to HUD Secretary Marcia L. Fudge, May 25, 2023, https://democrats-financialservices.house.gov/uploadedfiles/cmw_letter_hud_surveillance_tech_5.25.23_signed.pdf.
[525] U.S. Dep't of Housing and Urban Development, "Emergency/Natural Disaster and Safety/Security Funding," Mar. 13, 2024, https://www.hud.gov/program_offices/public_indian_housing/programs/ph/capfund/emfunding.
[526] HUD Statement, at 2.
[527] U.S. Dep't of Housing and Urban Development, "HUD Awards Nearly $10.4 Million to Public Housing Agencies for Safety and Security Needs," Oct. 4, 2022, https://web.archive.org/web/20230607233849/https://www.hud.gov/press/press_releases_media_advisories/hud_no_22_204.
[528] *See* Ewert Testimony, pp. 41-45.
[529] Douglas MacMillian, "Eyes on the poor: Cameras, facial recognition watch over public housing," *Washington Post*, May 16, 2023, https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/.
[530] Ibid.
[531] Ewert Statement, at 1.

> can be lost or stolen. Further, they share surveillance footage with local law enforcement agencies, claiming this deters crime and helps identify perpetrators.[532]

Considering the potential inaccuracies of FRT relating to race and gender discussed in the previous chapter,[533] the use of this technology is particularly consequential in subsidized housing, which has a disproportionate percentage of tenants of color and female tenants.[534] According to HUD, there are approximately 1.2 million households living in public housing units, managed by approximately 2,756PHAs.[535]

Emerging Civil Rights Concerns

In 2019, lawmakers sent a letter to HUD expressing concern over tenant allegations relating to the use of FRT and requested information about its deployment on federally assisted properties.[536] The letter asked how many federally assisted properties have used FRT in the last five years, whether federal funds were used to purchase FRT, whether residents have an opportunity to opt out of FRT, and what enforceable rules HUD has in place to ensure biometric data collected by the technology are kept secure.[537] Six months later, the Department responded that it was not aware of how many of its public housing programs use facial recognition or how it was being used.[538] Specifically, Len Wolfson, Assistant Secretary for Congressional and Intergovernmental Relations, wrote, "The Department does not monitor or track the use of facial recognition technology in federally-assisted properties."[539] The letter indicated that federal funds could have been used for facial recognition without disclosing it in requests and that "[i]n future years, the Department will request that PHAs indicate their intent to utilize facial recognition technology in conjunction with the security equipment purchased."[540] The Department also wrote that HUD has never conducted any research or implemented any policies on how facial recognition can be used in public housing, but that it encourages tenants to provide public comment on potential changes.[541]

In a joint statement, Senators Wyden (D-OR) and Booker (D-NJ) stated:

> It's obvious from this response that Housing and Urban Development has a lot of work to do to get a handle on whether facial recognition technology is being used on residents of public housing, who often have no choice in where they live or whether they will be subject to

---

[532] Ibid, at 2.
[533] *See, supra* notes 184-213.
[534] Ewert Statement, at 2.
[535] U.S. Dep't of Housing and Urban Development, "Public Housing," https://www.hud.gov/program_offices/public_indian_housing/programs/ph (accessed March 18, 2024). Exact number provided by HUD Affected Agency Review, Jun. 24, 2024.
[536] Letter to HUD Secretary Ben Carson, Dec. 18, 2019, https://www.wyden.senate.gov/imo/media/doc/121819%20Wyden-led%20letter%20to%20HUD%20RE%20facial%20recognition%20technologies.pdf.
[537] Ibid.
[538] Alfred Ng, "US government doesn't know how it uses facial recognition in public housing," *CNET,* Jun. 22, 2020, https://www.cnet.com/news/politics/us-government-doesnt-know-how-it-uses-facial-recognition-in-public-housing/.
[539] Ibid.
[540] Ibid.
[541] Ibid.

> invasive surveillance…HUD should conduct a thorough investigation into how many public housing authorities are using or are planning to use facial recognition and ban its use in public housing until there are ironclad assurances that it can be used without discriminating against Black, indigenous and other people of color.[542]

Property management companies employing FRT as a form of access control to buildings can also lead to discriminatory access practices. Director of the Washburn Law Clinic at Washburn University School of Law Michelle Ewert discussed how the technology is flawed due to inaccuracies in detecting individuals of various races, genders, and ages. This is especially problematic in subsidized housing, where tenants are "disproportionately women, disproportionately people of color and disproportionately seniors."[543] She described the tenants of Knickerbocker Village in New York, a housing development that has been using FRT for building access for over 10 years.[544] Ewert testified that the tenants, who are mostly of Chinese descent, "complain about the technology not recognizing them consistently, [and] having to stand outside in the rain and the cold because they can't get in."[545] Unfortunately, because HUD does not require its grantees to collect data relating to their use of FRT, it is unable to assess the extent to which these access systems are failing for tenants..

Michael Akinwumi, Chief Responsible AI Officer of the National Fair Housing Alliance, testified that "FRT's limitations in accurately recognizing faces from diverse racial and ethnic backgrounds can lead to disproportionate denials of access for underrepresented groups. This not only inconveniences residents but also sends a subtle message of exclusion."[546] Akinwumi maintains that use of FRT may constitute legally cognizable disparate impact if the technology is known to have higher misidentification rates for residents of certain racial backgrounds. He argued that "[w]hile the housing authority may cite enhanced safety and crime reduction as the justification for using this FRT, it is crucial to prove that these goals could not be achieved without measures carrying such a high risk of racial bias and intrusive surveillance."[547]

If HUD is providing funds for a technology known to have higher misidentification rates for minorities, and restricts their access to public housing, this could become a violation of these tenants' rights under Title VI.[548] Additionally, Akinwumi explained to the Commission that due to the fear of being constantly monitored, residents may refrain from exercising their First Amendment rights to free speech and association within their homes and community spaces.[549] Professor Ewert echoed these concerns and testified that tenants at the Atlantic Plaza Towers in New York alleged in a civil

---

[542] Ibid.
[543] Ewert Testimony, p.42.
[544] Ibid.
[545] Ibid.
[546] Akinwumi Statement, at 7.
[547] Ibid., at 10-11.
[548] *See, supra* notes 150-151.
[549] Akinwumi Statement, at 7.

rights complaint that "the landlord was pulling out screenshots of the tenants and sending it to them, basically trying to intimidate them to stop their tenant organizing."[550]

There are no data available for how often FRT purchased with HUD dollars is used for eviction. Of 41 housing authorities that told *The Washington Post* in 2023 they had bought new cameras using HUD grants in recent years, 11 indicated their systems had facial recognition tools and six indicated their intent to use its capabilities.[551] In an email to the *Post,* a Department spokesperson said there was never the intention for safety and security grants to be used to punish residents for lease violations, but that using FRT for those purposes was not a violation of grant terms.[552] There are also no regulations preventing a potential landlord from taking a photo of prospective tenants and selling that data to an FRT company. Landlords can also use an FRT database to screen applicants.[553] However, if the FRT was purchased with federal money and is being used in a discriminatory manner, Title VI's prohibition on using Departmental funds in a discriminatory manner would be violated.[554]

FRT raises significant privacy concerns among low-income tenants, as landlords and PHAs contract with AI companies to store residents' and their visitors' biometric data. The more entities that have access to sensitive and identifying data, the more vulnerable they are to a data security breach.[555] Professor Ewert explained that FRT in public housing creates a record of movements and associations, as if having an ankle monitor.[556] Ewert testified that:

> What is especially concerning about these privacy invasions is that low-income tenants have few options for affordable housing. If they forego rent-controlled units or subsidized housing, they are forced into the private rental market and face the likelihood of eviction if they can't consistently pay market-rate rent. While middle and upper-income people can choose whether to engage with surveillance technologies in their home, low-income tenants—disproportionately people of color—often do not have that freedom of choice. Or, more accurately, their choice is between privacy and housing.[557]

Because many low-income Americans have little choice in whether they need to reside in subsidized housing, granting consent to be subjected to FRT becomes a significant concern. Consumers using this type of housing do not have meaningful alternatives to submitting to the technology's surveillance, thus any "opt out" measures discussed among FRT regulations do not equally apply to those dependent on subsidized housing.[558] Ewert additionally raised a concern as to how FRT may interfere with personal relationships and key social support. As the technology surveils tenants as

---

[550] Ewert Testimony, p. 44.
[551] Douglas MacMillan, "Eyes on the poor: Cameras, facial recognition watch over public housing," *The Washington Post,* May 16, 2023, https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/.
[552] Ibid.
[553] Akinwumi Statement, at 9.
[554] *See, supra* notes 150-151.
[555] Ewert Statement, at 3.
[556] Ewert Testimony, p. 44.
[557] Ewert Statement, at 4.
[558] Ewert Testimony, pp. 70-72.

well as any guests and family members, people may be incentivized to not visit to avoid being captured by FRT and potentially misidentified or having their biometric data captured in a cyberattack.[559] This can lead to vulnerable tenants becoming disconnected from their social networks, "especially if the surveillance is being done in conjunction with law enforcement."[560]

Professor Michelle Ewert wrote in her statement to the Commission that HUD should take an additional administrative response to incorporate the restriction against purchasing FRT into all funding contracts and amend its contracts with housing providers to prohibit the use of automated surveillance and FRT regardless of funding source.[561] Alternatively, Ewert suggested that the agency should at least implement robust oversight including setting "clear parameters for use of these technologies, training for agency staff and housing providers on the technologies, and audits to ensure the technologies are reliable[,] and evaluate them for unintended, negative consequences on subsidized tenants."[562]

Following the April 2023 HUD notice, Congresswomen Maxine Waters and Ayanna Pressley sent a letter to HUD Secretary Marcia Fudge expressing concerns regarding about the usage of FRT in public housing.[563] The letter stated:

> [FRT] increases the ease and incidence of harassment of residents for committing minor community rule violations … we know that these technologies have a significant discriminatory impact that arises from identification errors related to individuals' skin color, gender, and age and other forms of bias built into these systems. This means that the likelihood that a resident of color will be blamed for a violation they did not commit increases substantially with the adoption of these technologies.[564]

Agency Efforts

As noted above, HUD issued a notice in April 2023 indicating that its Emergency Safety and Security Grant (ESSG) funds may not be used to purchase "automated surveillance and facial recognition technology."[565] This is the first time FRT was mentioned in a HUD grant notice,[566] three years after HUD's statement in 2020 that the Department would begin to request that PHAs indicate their intent

---

[559] Ibid., at 45.
[560] Ibid.
[561] Ewert Statement, at 5.
[562] Ibid.
[563] U.S. House Committee on Financial Services Democrats, "Ranking Member Waters, Congresswoman Pressley Urge HUD to Prohibit Use of Racially Biased Surveillance Technology in Federally Assisted Housing," May 26, 2023, https://democrats-financialservices.house.gov/news/documentsingle.aspx?DocumentID=410504.
[564] Ibid.
[565] U.S. Dep't of Housing and Urban Development, "Notice PIH 2023-10," Apr. 21, 2023, https://www.hud.gov/sites/dfiles/PIH/documents/2023PIH10.pdf.
[566] There is no mention of facial recognition technology in prior years of HUD ESSG notices. U.S. Dep't of Housing and Urban Development, "Notice PIH 2022-05," Mar. 10, 2022, https://www.hud.gov/sites/dfiles/PIH/documents/PIH2022-05.pdf; U.S. Dep't of Housing and Urban Development, "Notice PIH 2020-05," Sep. 17, 2020, https://www.hud.gov/sites/dfiles/PIH/documents/2020-25pihn.pdf; U.S. Dep't of Housing and Urban Development, "Notice PIH 2019-22," Aug. 19, 2019, https://www.hud.gov/sites/dfiles/PIH/documents/PIH-2019-22.pdf.

to utilize FRT in conjunction with security equipment purchased.[567] Additionally, the restriction applies only to *future* recipients of its security grants and does not limit the use of surveillance tools by authorities that have already purchased them.[568]

In HUD's response to the Commission's interrogatories and document requests, the Department stated that it has no regulations explicitly governing FRT use by program participants, and that:

> HUD does not require specific policies on FRT for Public Housing Authorities (PHA) and does not keep a list of PHAs that elect to use FRT. HUD's funds provide program participants the flexibility to purchase solutions and make investments that will provide decent, safe, and sanitary housing for residents.[569]

HUD wrote to the Commission that "[i]f a PHA misuses grant funds in violation of Federal, state, and local laws or HUD guidelines and regulations, HUD can issue the PHA a corrective action (opportunity to cure) with a 30-, 60-, 90-, or 120-day deadline to comply."[570] HUD did not provide information as to whether it had issued any corrective actions to a PHA regarding its use of FRT. Additionally, HUD stated that PHAs do not share any of their surveillance or FRT data or records with the Department.[571]

HUD stated that in addition to the 2023 modification to ESSG grants (i.e., making FRT a non-eligible purpose), it is exploring similar restrictions for other grant programs.[572] As of the writing of this report, it still may be possible for state and local government grantees to purchase FRT as part of an eligible activity, such as rehabilitation of a property, under HUD program statutes and regulations.[573]

HUD further indicated to the Commission that in an email on September 22, 2023, Principal Deputy Assistant Secretary Richard Monocchio advised PHAs to "find the right balance between addressing security concerns and respecting residents' right to privacy."[574] The email does not specifically mention FRT. It does, however, state HUD's position is that discontinuation of tenancy should only be pursued for serious violent behavior identified or multiple and serious violations of PHA leases—not mere minor offenses.[575]

Additionally, the Department stated:

> [HUD] requires that all program participants abide by Federal, state, and local laws as well as HUD guidelines and regulations. HUD requires this by collecting certifications and

---

[567] *See supra* note 540.
[568] Douglas MacMillan, "Eyes on the poor: Cameras, facial recognition watch over public housing," *The Washington Post,* May 16, 2023, https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/.
[569] U.S. Dep't of Housing and Urban Development, HUD Response to U.S. Commission on Civil Rights Interrogatories, Mar. 7, 2024.
[570] HUD Statement, at 2.
[571] Ibid.
[572] Ibid.
[573] Ibid, at 8.
[574] Ibid., at 2.
[575] U.S. Dep't of Housing and Urban Development, HUD Response to U.S. Commission on Civil Rights Interrogatories, Mar. 7, 2024, Supplemental.

> assurances from its recipients of HUD funding that they comply with various fair housing and civil rights requirements, including Title VI of the Civil Rights Act. HUD also requires, through its discretionary grant programs, that applicants agree to comply with these laws.[576]

The Commission requested that several representatives from HUD participate in the Commission's March 2024 briefing, but the Department declined to send any representatives. However, the Department did submit a written statement for the record following the briefing.

[576] U.S. Dep't of Housing and Urban Development, HUD Response to U.S. Commission on Civil Rights Interrogatories, Mar. 7, 2024.

[This page is left intentionally blank]

CHAPTER 3: The Federal Government's Efforts to Protect Civil Rights

The federal government, including the Executive branch and Congress, must ensure that their use of FRT use does not violate existing laws, including the Civil Rights Act and other anti-discrimination protections. As Deirdre Mulligan, Principal Deputy U.S. Chief Technology Officer of the White House Office of Science and Technology Policy (OSTP), wrote in her statement to the Commission:

> If we use this technology, we must use it responsibly—it needs to work, and it needs to protect people's rights, protect their freedoms, advance equity, and adhere to our fundamental obligation to ensure fair and impartial justice for all. Advances in technology have challenged us before. Each leap in capability brings new opportunities and, with them, new risks. Deciding how and when to use and refuse technology—including facial recognition technology—is a key way our nation manifests our values.[577]

As discussed in Chapters 1 and 2, without adequate oversight, sufficient training, regular auditing, and enforceable legal protections, the use of FRT can pose serious civil rights risks. The remainder of this report provides an overview of guidance established by the current Administration, as well as state and local efforts and proposed congressional legislation aiming to entrench civil rights within how the U.S. government uses FRT. The chapter concludes with proposed guidelines and oversight for best practices going forward, as FRT usage continues to expand across U.S. government agencies.

Executive Orders and White House and OMB Guidance

Executive Order 14074

In May 2022, President Biden signed Executive Order (E.O.) 14074, "Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety," which directed DHS, DOJ, and OSTP to identify privacy, civil rights, and civil liberties risks regarding the use of facial recognition technology. E.O. 14074 also directed DOJ, DHS, and OSTP to recommend best practices relating to the use of technology, including facial recognition and predictive algorithms.[578] According to the current Administration, the purpose of this E.O. is to promote accountability, transparency, and trust between law enforcement officials and the people they protect: the public.[579]

As discussed in Chapter 2, E.O. 14074 ordered DOJ to request the National Academy of Sciences (NAS) to conduct a study of facial recognition technology, "with a particular focus on the use of such technologies and algorithms by law enforcement, that includes an assessment of how such technologies and algorithms are used, and any privacy, civil rights, civil liberties, accuracy, or

---

[577] Mulligan Statement, at 1.
[578] Exec. Order No. 14074, *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety*, May 25, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/05/25/executive-order-on-advancing-effective-accountable-policing-and-criminal-justice-practices-to-enhance-public-trust-and-public-safety/
[579] *Id.*

disparate impact concerns raised by those technologies and algorithms or their manner of use."[580] The President ordered the NAS to publish a report on its findings, as well as its recommendations for the use of, or restrictions on, FRT. Additionally, E.O. 14074 ordered the Attorney General, the Secretary of Homeland Security, and the Director of OSTP to jointly lead an "interagency process" regarding the use of facial recognition technology by law enforcement agencies.[581] Pursuant to President Biden's order, the NAS released its FRT report in January 2024.[582] Several of these recommendations are discussed later in this chapter.

White House Blueprint for an AI Bill of Rights

In October 2022, the Biden White House published five principles to guide the design, use, and deployment of automated systems with the hope of protecting individuals from any threats that AI may pose. The principles laid out are:

- Safe and Effective Systems: protection from unsafe or ineffective systems
- Algorithmic Discrimination Protections: protection from discrimination by algorithms and systems, which should be used and designed in an equitable manner
- Data Privacy: protection from abusive data practices via built-in protections and agency over how data about the consumer is used
- Notice and Explanation: understanding when an automated system is being used and how and why it contributes to impactful outcomes
- Human Alternatives, Consideration, and Fallback: ability to opt out, where appropriate, and have access to a person that can consider, and remedy problems encountered.[583]

The Blueprint acknowledges the "extraordinary benefits" that automated systems have brought society but notes that this "important progress must not come at the price of civil rights or democratic values."[584]

The Blueprint indicates that continuous surveillance and monitoring should not be used in education, work, housing, or in other contexts where such surveillance is likely to limit rights, opportunities, or access.[585] As for the three Departments covered in this report, the enforcement of this Blueprint for an AI Bill of Rights could help mitigate some of the concerns about the continuous use of FRT monitoring in public housing.[586]

Executive Order 14110

---

[580] *Id.*
[581] *Id.*
[582] National Academies, "Advances in Facial Recognition Technology Have Outpaced Laws, Regulations; New Report Recommends Federal Government Take Action on Privacy, Equity, and Civil Liberties Concerns," Jan. 17, 2024, https://www.nationalacademies.org/news/2024/01/advances-in-facial-recognition-technology-have-outpaced-laws-regulations-new-report-recommends-federal-government-take-action-on-privacy-equity-and-civil-liberties-concerns.
[583] The White House Office of Science and Technology, *White House Blueprint Bill of AI Rights,* Oct. 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.
[584] Ibid.
[585] Ibid.
[586] *See supra* notes 536-560.

The following year, in October 2023, President Biden signed E.O. 14110, setting forth a government-wide approach to advancing and developing AI in a safe and responsible way. E.O. 14110 directs "over 50 federal entities to engage in more than 100 specific actions to implement the guidance set forth across eight overarching policy areas."[587] E.O. 14110 directs the Attorney General to meet with the heads of federal civil rights offices

> to discuss comprehensive use of their respective authorities and offices to: prevent and address discrimination in the use of automated systems, including algorithmic discrimination; increase coordination between the Department of Justice's Civil Rights Division and Federal civil rights offices concerning issues related to AI and algorithmic discrimination; improve external stakeholder engagement to promote public awareness of potential discriminatory uses and effects of AI; and develop, as appropriate, additional training, technical assistance, guidance, or other resources.[588]

Among other things, E.O. 14110 suggests providing training and technical assistance to "[s]tate, local, Tribal, and territorial investigators and prosecutors on best practices for investigating and prosecuting civil rights violations and discrimination related to automated systems, including AI."[589]

OMB Guidance

The Office of Management and Budget (OMB)'s mission is to assist the President in meeting policy, budget, management, and regulatory objectives, and oversees the implementation of the President's vision, including clearance of Presidential Executive Orders and memoranda to agency heads.[590] In November 2023, the month following President Biden's release of E.O. 14110, OMB released draft guidance on the development and use of AI while managing risks, with an emphasis on the safety and rights of the public.[591] The guidance was formally issued on March 28, 2024.[592] The guidance "establishes new agency requirements and guidance for AI governance, innovation, and risk management, including through specific minimum risk management practices for uses of AI that impact the rights and safety of the public."[593]

Specifically, the guidance states that, no later than December 1, 2024, agencies must follow the below practices *before* using new or existing covered safety-impacting or rights-impacting AI[594]:

---

[587] Exec Order No. 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,* Oct. 30, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.
[588] Exec. Order 14110, Sec.7 (ii).
[589] Exec. Order 14110, Sec.7 (iii).
[590] White House, "Office of Management and Budget," https://www.whitehouse.gov/omb/ (accessed Jun. 25, 2024).
[591] Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," Mar. 28, 2024, https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.
[592] Ibid.
[593] Ibid.
[594] OMB provides a list of safety-impacting and rights-impacting AI in Appendix I of the guidance. Ibid.

- Complete an AI impact assessment that documents the intended purpose and expected benefit, the potential risks, and the relevant data's quality and appropriateness. The expected benefits of the AI functionality should be considered against its potential risks, and if the benefits do not meaningfully outweigh the risks, agencies should not use the AI.
- Test the AI for performance in a real-world context. Such testing should follow domain-specific best practices, when available, and should take into account both the specific technology used and feedback from human operators, reviewers, employees, and customers who use the service or are impacted by the system's outcomes.
- Independently evaluate the AI using the Chief AI Officer (CAIO), and agency AI oversight board, or other appropriate agency office with existing test and evaluation responsibilities.

The guidance also clarifies that, by December 1, 2024 (and on an ongoing basis) while using new or existing covered safety-impacting or rights-impacting AI, agencies must:

- Conduct ongoing monitoring and establish thresholds for periodic human review at least annually, as well as after significant modifications to the AI or to the conditions or context in which the AI is used.
- Mitigate emerging risks to rights and safety, and where the AI's risks to rights or safety exceed an acceptable level and where mitigation is not practicable, agencies must stop using the affected AI as soon as is practicable.
- Ensure adequate human training and assessment. Training should be conducted on a periodic basis, determined by the agency, and should be specific to the AI use case, product, or service being operated.
- Provide appropriate human consideration as part of decisions that pose a high risk to rights or safety.
- Provide public notice and plain-language documentation through the AI use case inventory.[595]

Additionally, by December 1, 2024, agencies must follow certain minimum practices *before* initiating use of new or existing rights-impacting AI:

- Take steps to ensure the AI will advance equity, dignity, and fairness. This should include at least proactively identifying and removing factors contributing to algorithmic discrimination or bias, assessing and mitigating disparate impacts, and using representative data.
- Consult and incorporate feedback from affected groups, including underserved communities, in the design, development, and use of the AI, and use such feedback to inform agency decision-making regarding the AI.
- Conduct ongoing monitoring and mitigation for AI-enabled discrimination against protected classes that might arise from unforeseen circumstances, changes to the system after deployment, or changes to the context of use or associated data. Where sufficient mitigation is not possible, agencies must safely discontinue the use of the affected AI functionality.

[595] Ibid.

- Notify negatively affected individuals, with the notice including a clear and accessible means of contacting the agency and, where appropriate, requesting timely remediation for any related issues.
- Maintain human consideration and remedy processes by a fallback and escalation system in the event that an impacted individual would like to appeal or contest the AI's negative impact on them.
- Maintain options to opt out where practicable, where the affected people have a reasonable expectation of an alternative, or where lack of an alternative would meaningfully limit accessibility or create unwarranted harmful impact.[596]

Principal Deputy for OSTP Deirdre Mulligan stated in her written testimony to the Commission that this guidance is "the most prominent national policy anywhere in the world to affirmatively center civil rights in the design and use of technology by government."[597] She also indicated that without following the guidance laid out by OMB, agencies would "generally not be able to use" the technology.[598] Importantly, the guidance includes a section on waivers from minimum practices, stating:

> [A]n agency CAIO may waive one or more of the requirements in this section for a specific covered AI application or component after making a written determination, based upon a system-specific risk assessment, that fulfilling the requirement would increase risks to safety or rights overall or would create an unacceptable impediment to critical agency operations. An agency CAIO may also revoke a previously issued waiver at any time . . . CAIOs must centrally track waivers, reassess them if there are significant changes to conditions or context in which the AI is used, and report to OMB within 30 days of granting or revoking any waiver, detailing the scope, justification, and supporting evidence.[599]

Senior Policy Director of UnidosUS Laura MacCleery testified that these waivers may lead some of the more problematic deployments of FRT to continue, as agencies claim that law enforcement and national security exemptions apply or that an activity is "mission critical."[600] It was recommended that OMB create additional clarity regarding when agencies can seek waivers or exemptions.[601]

The OMB guidance includes many technical definitions, including "Artificial Intelligence Maturity" to refer to "a Federal Government organization's capacity to successfully and responsibly adopt AI into their operations and decision-making across the organization, manage its risks, and comply with

[596] Ibid.
[597] Mulligan Statement, at 3.
[598] Ibid.
[599] Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," Mar. 28, 2024, https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.
[600] MacCleery Statement, at 8.
[601] Ibid.

relevant Federal law, regulation, and policy on AI."[602] The OMB guidance, however, provides limited further explanation of some terms nor explains how these directives will be regulated and enforced, which could severely limit the impact of the guidance. In her written statement to the Commission, MacCleery stated:

> The task of the OMB Memo for the agencies is to establish "proper controls" over government uses of AI for current and near-future models and uses . . . the Memo is a solid start, but its approach is incomplete or lacks important clarity in a number of areas that could benefit from substantially more operational structure for agencies, and that OMB should more fully leverage the work of NIST. For example, the agencies' assignment under the Memo to achieve "maturity" for AI systems begs the question of how—and who—defines that success and on what grounds. Agencies will need constructive guidance on common technical issues arising from current uses and mitigations for AI systems, as well as to be informed about helpful developments and technical and sociotechnical challenges that arise in particular contexts and use cases. [603]

State and Local Efforts

In March 2023, the Connecticut Advisory Committee to the Commission investigated the use of AI across the state to determine what, if any, protections were in place to ensure that individuals' civil rights were being upheld. The report found that there was little transparency in the use of algorithms and data being relied upon. The report found that this lack of transparency raised concerns because some data sets are historically biased against people of color.[604] The Chair of the Committee stated that there is "very little public transparency around the government's use of algorithms here in Connecticut" and there are areas "where civil rights are really being implicated because they're potentially using algorithms that are either using data sets that are clogged, or the algorithms themselves are set up in ways that are perpetually biased. We have to get ahead of that before they proliferate our state."[605] Following the release of the bipartisan approved report in June 2023, the Connecticut General Assembly unanimously passed a bill.[606] The new law will establish a 21-

[602] Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," Mar. 28, 2024, https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.
[603] MacCleery Statement, at 6.
[604] Connecticut Advisory Committee to the U.S. Commission on Civil Rights, "The Civil Rights Implications of Algorithms," Mar. 2023, https://www.usccr.gov/files/2023-04/ct-sac-algorithm-report.pdf.
[605] Emilia Otte, "CT Seeks Stricter AI Regulations After Federal Report Suggests Algorithm Bias," *CT Examiner*, Apr. 26, 2023, https://ctexaminer.com/2023/04/26/ct-seeks-stricter-ai-regulations-after-federal-report-suggests-algorithm-bias/.
[606] Hugh McQuaid, "Senate Passes Proposal to Review AI in State Government," *CT News Junkie*, May 12, 2023, https://ctnewsjunkie.com/2023/05/12/senate-passes-proposal-to-review-ai-in-state-government/; Christine Stuart, "House Joins Senate In Regulating AI in State Government," *CT News Junkie*, May 30, 2023, https://ctnewsjunkie.com/2023/05/30/house-joins-senate-in-regulating-ai-in-state-government/.

member working group to inform future regulations on AI use, draft a Connecticut AI Bill of Rights, and establish policies to govern private sector use of AI.[607]

Some states have worked to fill the gaps in protections against facial recognition technology specifically. Other states have expressly prohibited or limited the use of FRT by government entities.[608] Some states have also enacted laws limiting private industry's collection and use of biometric information.[609] Others have prohibited private entities from profiting off consumer biometric or genetic information, creating requirements to maintain publicly available written policies on biometric data retention and destruction.[610]

Most notably, Illinois passed a biometric privacy law, the Illinois Biometric Information Privacy Act (BIPA), in 2008.[611] BIPA regulates "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information," defining "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[612] BIPA created a private right of action and the ability to litigate against companies, which have forced changes to controversial business practices, such as stopping Clearview AI from selling its face surveillance system to private companies,[613] and making way for large consumer class action lawsuits.[614] Many states have since passed laws similar to BIPA.[615]

---

[607] An Act Concerning Artificial Intelligence, Automated Decision-Making, and Personal Data Privacy, S.B. 1103, (2023), https://legiscan.com/CT/text/SB01103/2023.

[608] Cong. Rsch. Serv., R46541, Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations 9 n.80 (2020) https://crsreports.congress.gov/product/pdf/R/R46541 (citing N.H. REV. STAT. § 263:40-b ("The department [of motor vehicles] is prohibited from using any facial recognition technology in connection with taking or retaining any photograph or digital image for purposes of this chapter."); OR. REV. STAT. § 133.741 (barring "the use of facial recognition or other biometric matching technology to analyze recordings obtained" via body cameras worn by state and local police); WASH. REV. CODE ANN. § 43.003.0011 (effective July 21, 2021) (limiting the use of FRT by state or local governments "to engage in on going surveillance, conduct real-time or near real-time identification, or start persistent tracking" except in enumerated circumstances).

[609] Cong. Rsch. Serv., R46541, Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations 9 n.81 (2020) https://crsreports.congress.gov/product/pdf/R/R46541 (citing ILL. COMP.STAT. 14/1; TEX. BUS. & COM. CODE § 503.001; ALASKA STAT. § 18.12.010).

[610] Cong. Rsch. Serv., R46541, Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations 9 n.83 (2020) ps://crsreports.congress.gov/product/pdf/R/R46541 (citing CAL. CIV. CODE §§ 1798.100–1798.199; TEX. BUS. &COM. CODE § 503.001; WASH. REV. CODE §§ 19.375 et seq.).

[611] ILL. COMP. STAT. 14/1 et seq.

[612] Cong. Rsch. Serv., R46541, Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations 9 (2020) https://crsreports.congress.gov/product/pdf/R/R46541; ILL. COMP. STAT. 14/10 § 5(g); ILL. COMP. STAT. 14/10 § 10.

[613] Caitriona Fitzgerald, Kara Williams & R.J. Cross, The State of Privacy: How state "privacy" laws fail to protect privacy and what they can do better, Electronic Privacy Information Center (EPIC) & U.S. PIRG Education Fund 18 (Feb. 2024) https://epic.org/wp-content/uploads/2024/01/EPIC-USPIRG-State-of-Privacy.pdf; *see* Ryan Mac & Kashmir Hill, Clearview AI Settles Suit and Agrees to Limit Sales of Facial Recognition Database, N.Y. Times (May 9, 2022), https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html.

[614] Cong. Rsch. Serv., R46541, Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations 9-10 (2020) https://crsreports.congress.gov/product/pdf/R/R46541 (citing Class Action Complaint, Carmine v. Macy's Retail Holdings, Inc., No. 20-cv-4589 (N.D. Ill. Aug. 5, 2020), Class Action Complaint, Whalen v. Facebook, Inc., No. 20-CIV-03346 (Cal. Superior Court, San Mateo Aug. 10, 2020)).

[615] TEX. BUS. & COM. CODE § 503.001; WASH. REV. CODE §§ 19.375.010–19.375.900; CAL. CIV. CODE §§ 1798.100–1798.199.

Municipalities have also responded to the spread of FRT usage. San Francisco, California became the first city in the country to ban the use of facial recognition technology by a municipal government agency in May 2019.[616] Under the city's administrative code, it became unlawful for any public agency to "obtain, retain, access, or use" any FRT on "city-issued software or a city-issued product or device" or to obtain any information from FRT.[617] Starting in 2016, the ACLU has been active in promoting a model bill for local governments interested in regulating surveillance technology. The Community Control Over Police Surveillance (CCOPS) is a model bill that requires city council approval before purchasing new surveillance technology.[618] As of 2023, at least 22 local governments have adopted surveillance technology regulations using the ACLU model as a template.[619] One such city, Sommerville, Massachusetts, worked with the ACLU to pass an ordinance requiring transparency in the city's purchase and use of new surveillance technology, and then went on to unanimously pass a facial recognition ban.[620] Oakland, California, has often been cited as a model for local governance of surveillance technologies, enacting technology regulations and creating a separate advisory commission to share responsibility with the City Council on privacy concerns.[621] In June 2024, the City of Detroit settled with Robert Williams following a wrongful arrest following a false FRT match.[622] The settlement includes prohibiting police from arresting people based solely on FRT results or photo lineups following a facial recognition search, mandating training on FRT, and requiring an audit of all cases in which FRT was used to obtain an arrest warrant since 2017.[623]

Following a 2020 *New York Times* article critical of law enforcement's use of FRT,[624] the Miami Police Department voluntarily set out to establish an FRT policy that would address balancing privacy concerns with utility in criminal investigations. Armando Aguilar, Assistant Chief of the

---

[616] Kate Conger, Richard Fausset and Serge F. Kovalesk, "San Francisco Bans Facial Recognition Technology," *The New York Times,* May 14, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.
[617] National Academies of Sciences, Engineering, and Medicine, Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance 70 (The National Academies Press, 2024) https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance (citing M. Fidler, 2020, "Local Police Surveillance and the Administrative Fourth Amendment," Santa Clara Computer and High Technology Law Journal, Aug 2, p. 546, http://dx.doi.org/10.2139/ssrn.3201113.).
[618] Community Control Over Police Surveillance (CCOPS) Model Bill, ACLU (Apr. 2021) https://www.aclu.org/documents/community-control-over-police-surveillance-model-bill.
[619] Community Control Over Police Surveillance (CCOPS), ACLU https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance (accessed Mar. 13, 2024).
[620] Sarah Wu, Summerville City Council Passes Facial Recognition Ban, Boston Globe (Jun. 27, 2019) https://www.bostonglobe.com/metro/2019/06/27/somerville-city-council-passes-facial-recognition-ban/SfaqQ7mG3DGulXonBHSCYK/story.html; New Somerville Policy First in MA to Add Controls, Require Public Transparency for Surveillance Technology, City of Summerville (Oct. 5, 2017) https://www.somervillema.gov/news/new-somerville-policy-first-ma-add-controls-require-public-transparency-surveillance-technology.
[621] Oakland, CA., Code § 9.64.045; National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.
[622] Steve Neavling, "Detroit police to overhaul facial recognition use after 'groundbreaking settlement' in false arrest suit," *Detroit Metro Times*, Jun. 28, 2024, https://www.metrotimes.com/news/detroit-police-to-overhaul-facial-recognition-use-after-groundbreaking-settlement-in-false-arrest-suit-36657192.
[623] Ibid.
[624] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times,* Jan. 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Miami Police department, testified that his team met with local privacy advocates, took recommendations, incorporated some of them into policies, and even held virtual town hall meetings.[625] Aguilar informed the Commission that:

> The policy which resulted from our efforts created a narrow framework within which we would come to use FR [face recognition]. Most importantly, our policy emphasizes that FR matches do not constitute probable cause to arrest. Matches are treated like anonymous tips, which must be corroborated by physical, testimonial, or circumstantial evidence. We laid out five allowable uses: criminal investigations; internal affairs investigations; and identifying cognitively impaired persons, deceased persons, and lawfully detained persons.
>
> We use FR retrospectively, i.e., we do not use it on a "live" or "real time" basis to identify persons going about their business in public spaces, and we do not use it to identify persons who are carrying out constitutionally protected activities. We established a policy limiting who has access to our FR platforms, we disclose our use of FR to defense counsel in criminal cases, and we do not substantively manipulate or alter probe photographs, use composite sketches as probe photographs, or use any other technique which has not been scientifically validated.[626]

While these individual efforts are a good step to ensure individuals' civil rights are being upheld, there are existing federal civil rights laws that Departments have an obligation to enforce, including the requirement to respond if FRT use results in negative outcomes that have a disparate impact on protected classes. Federal guidance establishing proper measures and boundaries regarding the utilization of FRT is paramount, since state and local entities may look to federal models and standards to adopt at the state level.

Proposed Federal Legislation

Over the past several years, there have been a number of proposed Congressional bills regarding FRT that could affect how the three agencies in this report utilize the technology. Several of these bills are bipartisan in nature which highlights the importance of addressing potential civil rights concerns for the American people when it comes to the development and deployment of FRT by federal agencies.

In June 2022, Representative Donald Beyer (D-VA) introduced the Facial Recognition Ban on Body Cameras Act, to establish a framework to prohibit federal, state, and local law enforcement agencies from using facial recognition technology on images captured by body-worn cameras.[627] Specifically, the bill prohibits federal law enforcement agencies from using facial recognition technology or other remote biometric surveillance systems on any image acquired by body-worn cameras of law

[625] Armando Aguilar, Assistant Chief, Miami Police Department, Written Statement for the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, at 2 (hereinafter Aguilar Statement).
[626] Aguilar Statement, at 2-3.
[627] H.R.8154 - Facial Recognition Ban on Body Cameras Act, https://www.congress.gov/bill/117th-congress/house-bill/8154.

enforcement officers.[628] Additionally, the bill requires state and local governments to comply with a similar law or policy as a condition of receiving funds under the Edward Byrne Memorial Justice Assistance Grant (JAG) program.[629] Beyer proposed the bill stating that "[o]nce-futuristic technologies, like FRT and biometric tools, are now increasingly in use by law enforcement in American communities, but Congress is woefully behind in considering the implications of their deployment for civil liberties."[630]

In September 2023, Senators Richard Blumenthal (D-CT) and Josh Hawley (R-MO), Chair and Ranking Member of the Senate Judiciary Subcommittee on Privacy, Technology, and the Law respectively, announced a bipartisan legislative framework to establish guardrails for artificial intelligence.[631] The framework lays out specific principles for upcoming legislative efforts, including the establishment of an independent oversight body, ensuring legal accountability for harms, defending national security, promoting transparency, and protecting consumers and children.[632] The announcement followed multiple hearings in the Subcommittee featuring witness testimony from industry and academic leaders.[633]

In September 2023, Representative Yvette Clarke (D-NY) introduced the No Biometric Barriers to Housing Act of 2023, which would prohibit the usage of facial and biometric recognition technology in most federally funded public housing and require HUD to submit a comprehensive report to Congress about how the technology impacts the public housing sector and its tenants.[634] In her written statement to the Commission, Congresswoman Clarke stated:

> Public housing exists to provide shelter for our constituents, not to create yet another opportunity to be wrongly profiled. We simply cannot allow technology and innovation to undermine tenants' civil liberties or their quality of life. We cannot be forced to choose between the promise of innovation and the sanctity of civil rights. Those who cannot afford more do not deserve less in basic privacy and protection. They should not have to compromise their civil rights and liberties nor accept the condition of indiscriminate, sweeping government surveillance to find an affordable place to live.[635]

It should be noted that while this proposed legislation would offer strong protections relating to FRT to certain subsidized tenants, it does not offer protections to tenants with Housing Choice Voucher

---

[628] Ibid.
[629] H.R.8154 - Facial Recognition Ban on Body Cameras Act, https://www.congress.gov/bill/117th-congress/house-bill/8154.
[630] Congressman Don Beyer, "Beyer, Lieu Reintroduce Legislation To Block Law Enforcement From Using Facial Recognition Technology With Body Cam Footage," Jun. 21, 2022, https://beyer.house.gov/news/documentsingle.aspx?DocumentID=5619.
[631] Sen. Richard Blumenthal [D-CT], "Blumenthal & Hawley Announce Bipartisan Framework on Artificial Intelligence Legislation," Sept. 8, 2023, https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-and-hawley-announce-bipartisan-framework-on-artificial-intelligence-legislation
[632] Ibid.
[633] Ibid.
[634] Congresswoman Yvette D. Clarke, "Clarke introduces legislation to ban usage of facial recognition & biometric identification technology in public housing," Sept. 8, 2023, https://clarke.house.gov/clarke-introduces-legislation-to-ban-usage-of-facial-recognition-biometric-identification-technology-in-public-housing/.
[635] Clarke Statement, at 3.

Program (HCVP) vouchers, who far outnumber public housing residents.[636] To provide long-term protections to a majority of subsidized tenants, the legislation would need to be expanded to cover additional housing programs.[637]

In October 2023, Representative Ted Lieu (D-CA) introduced the Facial Recognition Act of 2023.[638] The legislation places strong limits on law enforcement use of FRT, provides transparency, and requires annual assessments and reporting on the deployment of the technology to protect individuals' rights.[639] Specifically, the bill requires that a warrant be obtained that shows probable cause that an individual committed a serious violent felony before FRT is deployed.[640] In his written statement to the Commission, Congressman Lieu stated that "In placing strong limits and prohibitions on use of FRT, law enforcement will be able to harness the benefits of this powerful technology while curbing potential misuse and abuse."[641] The Facial Recognition Act of 2023 would limit law enforcement use of FRT to situations in which a warrant is obtained that shows probable cause an individual committed a serious violent felony; the Act requires law enforcement to provide individuals subject to an FRT search with notice and a copy of the court order and/or other key data points.[642] Lieu concludes in his testimony that "[t]he bipartisan success of state regulatory bills bodes well for such an approach at the federal level. We need to build robust safeguards that provide transparency to the American people, prevent discriminatory algorithms, ensure defendants are protected with due process rights, and limit the use of the technology to only necessary cases. The Facial Recognition Act is an approach we can build on."[643]

In November 2023, Senator Jeff Merkley (D-OR) joined with Senators John Kennedy (R-LA), Edward J. Markey (D-MA), Roger Marshall (R-KS), Bernie Sanders (I-VT), and Elizabeth Warren (D-MA) to introduce the Traveler Privacy Protection Act of 2023.[644] The bipartisan Traveler Privacy Protection Act would prevent TSA from using airports as a site to collect Americans' facial biometric data by:

- Repealing existing authorization for TSA to explore facial recognition technology and require explicit congressional authorization for future use.
- Immediately banning TSA from expanding its use of facial recognition.

---

[636] Ewert, M. Y. (2022) "The Dangers of Facial Recognition Technology in Subsidized Housing," *J. Legis. & Pub. Pol'y 665*, https://ssrn.com/abstract=4216859.
[637] Ibid.
[638] H.R.6092 - Facial Recognition Act of 2023, https://www.congress.gov/bill/118th-congress/house-bill/6092.
[639] Rep. Ted Lieu, "Reps Lieu, Jackson Lee, Clarke, Gomez, Ivey, and Veasey Introduce Bill to Regulate Law Enforcement's Use of Facial Recognition Technology," Oct. 27, 2023, https://lieu.house.gov/media-center/press-releases/reps-lieu-jackson-lee-clarke-gomez-ivey-and-veasey-introduce-bill.
[640] Ibid.
[641] Lieu Statement, at 5.
[642] Ibid., at 5-6.
[643] Ibid., at 7.
[644] Senator Jeff Merkley, "In Midst of Busy Travel Season, Merkley, Kennedy, Colleagues Sound Alarm on TSA Collection of Facial Biometric Data," Nov. 29, 2023, https://www.merkley.senate.gov/in-midst-of-busy-travel-season-merkley-kennedy-colleagues-sound-alarm-on-tsa-collection-of-facial-biometric-data/.

- Requiring TSA to end its facial recognition program and dispose of facial biometrics data within 3 months.[645]

Senator Roger Marshall (R-KY) stated that he signed onto the bill because he is:

> concerned that we have no clue where this data is going, and thousands of Americans every day are not aware of their option to decline to have their photo taken by a government agency every time they go to the airport. The potential for these images to be used to violate American's civil liberties is greatly concerning. Our important bipartisan legislation would put a halt to the expansion of this facial recognition program and involve Congress in the future use of it. I'm proud to work with Senators Merkley and Kennedy to protect Americans and force transparency from the TSA.[646]

Critics of the legislation argue it may increase security threats. Sheldon Jacobson, Professor of Computer Science at the University of Illinois at Urbana-Champaign, stated that "This bill is a threat to our national security, having the unintended consequence of empowering bad actors with malicious intents to infiltrate and disrupt the nation's air system, increasing the risk to all Americans who travel by air."[647]

In April 2024, the House of Representatives passed the "Fourth Amendment Is Not For Sale Act," introduced by Representative Warren Davidson (R-OH).[648] The bill, in part, "limits the authority of law enforcement agencies and intelligence agencies to access certain customer and subscriber records or illegitimately obtained information. With respect to such records, the bill prohibits law enforcement agencies and intelligence agencies from obtaining the records or information from a third party in exchange for anything of value (e.g., purchasing them); prohibits other government agencies from sharing the records or information with law enforcement agencies and intelligence agencies; and prohibits the use of such records or information in any trial, hearing, or proceeding."[649] The bill indicates that if the government wants to access protected data, it must obtain a warrant beforehand. If found to apply to FRT usage, the bill could implicate how agencies are currently operating FRT systems.

In May 2024, Senator Jeff Merkley (D-OR) submitted an amendment to the bill reauthorizing the Federal Aviation Administration (FAA) through 2028.[650] The key purpose of the amendment was to prohibit the expansion of facial recognition technology within the TSA. In a letter to Majority Leader Schumer and Minority Leader McConnell, Senator Merkley, along with several other Senators, wrote about their concern regarding TSA's existing use of FRT and eventual requirement for

---

[645] Ibid.
[646] Ibid.
[647] Sheldon H. Jacobson, "The Traveler Privacy Protection Act is a threat to our national security," *The Hill,* Dec. 1, 2023, https://thehill.com/opinion/technology/4337073-the-traveler-privacy-protection-act-is-a-threat-to-our-national-security/.
[648] H.R.4639 - Fourth Amendment Is Not For Sale Act, https://www.congress.gov/bill/118th-congress/house-bill/4639.
[649] Ibid.
[650] S.Amdt.2000 to H.R.3935, https://www.congress.gov/amendment/118th-congress/senate-amendment/2000.

biometrics to be used "across the board."[651] The Senators highlighted that the 2024 Federal Aviation Administration Reauthorization is an opportunity for Congress to address the issue of widespread biometric use in the TSA and to "provide needed oversight of TSA's facial recognition program." The Senators cautioned that "[s]hould Congress delay, TSA's facial recognition infrastructure will soon be in place at hundreds of cities across America, and it will be that much more difficult to rein in facial recognition surveillance by the federal government."[652] This amendment to the bill was unsuccessful.[653]

Proposed Guidelines for Best Practices

The NAS published its study report on facial recognition in January 2024.[654] The report provides suggested guidelines to mitigate potential harms as well as foster trust and mitigate biases. The NAS recommended that the federal government take prompt action to sustain a vigorous program of FRT testing and evaluation, establish industry-wide standards, and multi-disciplinary working groups to develop and periodically review standards for reasonable and equitable use.[655] There is also a need for standards across the disciplines utilizing FRT. As Katie Kinsey of Policing Project stated in her testimony:

> The absence of standards pervades the entire pipeline – from the designers and developers of the core technology to law enforcement agency policies to training for the officers and prosecutors who rely on the technology. This choose-your-own-adventure approach makes no sense. A policing agency using FRT in Wichita, Kansas has the same interest in system accuracy and data security protection as does the LAPD. Similarly, best practices for reducing cognitive biases from human review of FRT results should guide the use of the technology no matter the jurisdiction.[656]

The NAS also indicated that the federal government should establish a program to develop and refine a risk management framework to help organizations identify and mitigate the risks of proposed facial recognition technology applications regarding performance, equity, privacy, civil liberties, and effective governance.[657]

---

[651] Senator Merkley, Letter to Sen. Majority Leader and Sen. Minority Leader, Re: Restricting Use of Facial Recognition Technology by TSA, May 2, 2024, https://www.merkley.senate.gov/wp-content/uploads/2024_05_02_LTR-TSA-Freeze-to-Leadership.pdf.
[652] Ibid.
[653] Edward Graham, "Senate passes FAA reauthorization without TSA biometrics amendment," *NextGov,* May 10, https://www.nextgov.com/emerging-tech/2024/05/senate-passes-faa-reauthorization-without-tsa-biometrics-amendment/396486/. 2024,
[654] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.
[655] Ibid.
[656] Kinsey Statement, at 9.
[657] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.

In January 2023, NIST released the AI Risk Management Framework, developed through a consensus-driven, open, transparent, and collaborative process that included a Request for Information, several draft versions for public comments, multiple workshops, and other opportunities to provide input.[658] It is intended to build on, align with, and support AI risk management efforts by others.[659] It did not, however, provide a numerical recommendation as far as accuracy risk for FRT algorithms. Nicol Turner Lee, Senior Fellow at the Brookings Institute and contributor to NAS's FRT report, wrote in her statement to the Commission that "despite several years of research, there is still no agreed upon definition of algorithmic fairness."[660]

The NAS recommended the government support research to improve the accuracy and minimize demographic biases of current and potential FRT uses.[661] Brian Finch of Pillsbury Law wrote in his statement to the Commission that "federal procurements of FRTs and federal grant funds being spent on FRTs should only be allowed when FRVT [Face Recognition Vendor Test] results indicate that the algorithm used in the FRT has a false-positive rate below a certain threshold" – thus the government should set a maximum acceptable error rate across various demographic groups when considering federal procurement of 1:N algorithms.[662] Similarly, NAS called for requiring federal grant recipients to adopt minimum standards for the quality of probe and reference gallery images, use FRT systems that present only candidates who meet a minimum similar threshold, and return zero matches if no candidates meet that threshold.[663]

Michael Akinwumi, Chief Responsible AI Officer of the National Fair Housing Alliance wrote that the Commission should urge Congress to mandate comprehensive training on technology and AI bias for federal regulators and enforcement agencies, and strongly emphasize the implementation of fair housing and racial equity principles.[664] Akinwumi asserts that there should be a push for the allocation of resources to ensure federal agencies have the equipment and personnel needed for rigorous testing and oversight of technologies that have the potential for discriminatory impact.[665]

The NAS report also recommended that DOJ and DHS establish an FRT working group to develop and review standards for reasonable and equitable use, as well as other needed guidelines for FRT

---

[658] NIST, "AI Risk Management Framework," https://www.nist.gov/itl/ai-risk-management-framework (accessed Mar. 27, 2024).
[659] Ibid.
[660] Turner Lee Statement, at 19.
[661] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.
[662] Brian Finch, Attorney, Pillsbury Winthrop Shaw Pittman LLP, Written Statement for the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, at 10 (hereinafter Finch Statement).
[663] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.
[664] Akinwumi Statement, at 15.
[665] Ibid.

use by federal, state, and local law enforcement agencies.[666] Authors of the report stated that the working group should be charged with developing minimum technical requirements for FRT procured by law enforcement agencies and a process for periodically evaluating and updating the standards.[667] This would consist of developing requirements for the training and certification of officers and staff using FRT as well as establishing requirements for documentation and auditing.[668] Beyond merely setting standards, Dr. Heather Roff, Associate Fellow, Leverhulme Centre for the Future of Intelligence, University of Cambridge and Senior Research Scientist, Center for Naval Analysis explained that there is need to engender "a culture of responsible use."[669] She testified that:

> Compliance based approaches that look to "trickle down" compliance through the typical annual training done by large agencies (cybersecurity, privacy, ethics and compliance, etc.) will not provide adequate education and guidance to those working with FRTs in law enforcement.[670]

The Center for Democracy and Technology has also recommended that federal law enforcement officers investigating a crime limit the use of facial recognition to situations in which there is probable cause to believe that an unidentified individual to be scanned has committed the crime.[671] As discussed in Chapter 2, law enforcement may not disclose information on the use of FRT in discovery materials that are used for the defense.[672] Law enforcement should develop policies to ensure that defendants receive notification on use of facial recognition technology, as well as all pertinent information about its use.[673]

K.J. Bagchi from The Leadership Conference stressed to the Commission that, despite the accessibility provisions called for in E.O. 14110[674] (discussed above), individuals with disabilities continue to face significant challenges when using AI systems. He testified that:

---

[666] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.
[667] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.
[668] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.
[669] Heather Roff, Associate Fellow, Leverhulme Centre for the Future of Intelligence, University of Cambridge and Senior Research Scientist, Center for Naval Analysis, Written Statement for the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, at 8 (hereinafter Roff Statement).
[670] Roff Statement, at 8-9.
[671] Center for Democracy & Technology, "Transparency and Policy Recommendations for Federal Law Enforcement Use of Facial Recognition," Jan. 19, 2024, https://cdt.org/wp-content/uploads/2024/01/DOJ-DHS-Comment-Transparency-and-Policy-Recommendations-for-Federal-Law-Enforcement-Use-of-Facial-Recognition.pdf.
[672] *See, supra* notes 221-223.
[673] Center for Democracy & Technology, "Transparency and Policy Recommendations for Federal Law Enforcement Use of Facial Recognition," Jan. 19, 2024, https://cdt.org/wp-content/uploads/2024/01/DOJ-DHS-Comment-Transparency-and-Policy-Recommendations-for-Federal-Law-Enforcement-Use-of-Facial-Recognition.pdf.
[674] Exec. Order 14110.

> Agencies need to intentionally include people with disabilities by building systems that conform to accessibility standards. Agencies should also consider the impact that differences in language may have to ensure accessibility for the communities where AI systems are used.[675]

Several civil rights organizations have called for the suspension or banning of FRT use while its potential harms remain unquantified.[676] However, Armando Aguilar, Assistant Chief of Miami Police Department, explained how he weighs the issues of FRT use by police:

> The public is right to be leery of FRT, as they should be with any other emerging technology. But if there were just two key points that I could convey to critics of FRT it would be the following: 1) law enforcement and the public can work together to create responsible FRT policy, and 2) if not FRT (or AI, more broadly), then what?[677]

He concludes that FRT allows law enforcement to solve crimes that would otherwise go unsolved and allows an investigation to focus on drivers of violent crime as opposed to casting a wide net on entire communities affected by crime.[678]

The NAS report also stated that policies and procedures should address law enforcement failures to adhere to procedures or to attain appropriate certification, and mechanisms for redress by individuals harmed by misuse or abuse of FRT.[679] Nicol Turner Lee, Senior Fellow at the Brookings Institution, testified that:

> When individuals and their families are harmed or have had their rights breached by FRT, the government must enable either through legislation, or the actions of State Attorney Generals some form of remuneration and/or appeal for affected individuals to recover from the resulting reputational and financial consequences of FRT, especially when violations are made under the direction of the government when it is designing, deploying, licensing and/or distributing AI, and more specific algorithmic models that lead to potentially irreversible harms.[680]

To foster trust, NAS recommended that institutions developing or deploying FRT should take steps to cultivate greater community trust by adopting more inclusive designs and engaging with

---

[675] Koustubh **"**K.J." Bagchi, Vice President, Center for Civil Rights and Technology, The Leadership Conference, Written Statement for the Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing before the U.S. Comm'n on Civil Rights, Mar. 8, 2024, at 8 (hereinafter Bagchi Statement).
[676] *See* Baghchi Testimony, pp. 220-221; Fight for the Future, Public Comment, Apr. 8, 2024 [on file]; Electronic Privacy Information Center (EPIC), Public Comment, Apr. 8, 2024 [on file]; Surveillance Technology Oversight Project (S.T.O.P.), Public Comment, Apr. 8, 2024 [on file].
[677] Armando Aguilar, Assistant Chief, Miami Police Department, Response to Follow-Up Questions, p. 1 [on file].
[678] Ibid.
[679] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.
[680] Turner Lee Statement, at 2.

communities to help individuals understand the technology's capabilities, limitations, and risks.[681] In addition to developers, governments can give impacted communities a voice in the process that provides a means of feedback about the uses and impacts of technologies in real time.[682]

The NAS suggested that to enact more comprehensive safeguards, the Executive Office of the President could consider issuing an executive order on the development of guidelines for the appropriate use of facial recognition technology by federal departments and agencies and addressing equity concerns and the protection of privacy and civil liberties.[683] Additionally, new legislation should consider ways to address equity, privacy, and civil liberties concerns raised by facial recognition technology, to limit harms to individual rights by both private and public actors, and to protect against its misuse.[684] Potential legislation could also consider limitations on the storage of face images and templates for prescribed government functions (such as at the border or at international travel points), where explicit consent for a specific purpose is given (such as consenting to use FRT to unlock a smartphone), and where there are threats to life and physical safety.[685] The recommendations conclude, "FRT is a powerful tool with profound societal implications. It will be critically important to adopt a considered approach to its governance and future development."[686]

[681] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.
[682] MacCleery Statement, at 9.
[683] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Jan. 2024, https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.
[684] Ibid.
[685] Ibid.
[686] Ibid.

[This page is left intentionally blank]

CHAPTER 4: Findings and Recommendations

Glossary

- **Civil Rights Act of 1964:** outlaws discrimination in public places, provides for the integration of schools and public facilities, makes discrimination in employment illegal, bans the unequal application of voter registration requirements, and prohibits discrimination by federal funding recipients.
    - **Title VI:** "No person in the United States shall, on the ground of race, color, or national origin, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving Federal financial assistance."
- **Privacy Act of 1974:** prohibits the disclosure of records containing personally identifiable information about an individual without the written consent of the individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with the means to access and to amend their records**.**
- **E-Government Act of 2002:** requires all Federal government agencies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form to create Privacy Impact Assessments (PIAs) and to make them available to the general public unless the PIA is subject to an exemption.

Findings

I. Overview

a. The U.S. currently does not have a coherent national AI use strategy, despite a recent Executive Order instructing the development of guidelines and best practices for AI safety and security.

b. FRT is used by DOJ, DHS, and HUD, as well as their funding recipients, in several programs across the FBI, TSA, CBP, and public housing agencies. While DOJ recently adopted an interim FRT policy, and DHS published a Department-wide FRT directive, HUD does not track FRT use.

II. Facial Recognition Technology, Civil Rights, and Constitutional Rights

a. There are currently no federal laws or regulations that expressly authorize or limit FRT use by the federal government.

b. Title VI authorizes and directs federal departments and agencies that extend financial assistance to issue rules, regulations, and orders that effectuate Title VI's prohibition on discrimination on the bases of race, color, and national origin. DOJ, DHS, and HUD have promulgated their own regulations under Title VI.

c. Two major statutes also govern the collection and use of personal information by a federal agency: the Privacy Act of 1974 and the E-Government Act of 2002. Neither act directly addresses FRT, however, they do place limits on how agencies collect, store, and use information directly and through partnerships with private parties and state and local governments.

III. Federal Use

a. While there are interim policies for FRT use, as of July 2024, there is no official, standardized policy published for FRT use. Nonetheless, FRT is being used for one or more purposes across several agencies throughout the federal government, including those that employ law enforcement officers.
b. In testimony to the Commission, the Government Accountability Office (GAO) indicated that, at the time of its 2019-2022 investigation into federal law enforcement use of FRT, agencies falling under the DOJ and DHS, including the FBI and CBP, did not have guidance or policies specific to FRT that addressed civil rights and civil liberties. In September 2023, DHS published a Department-wide FRT directive. In December 2023, DOJ established an interim FRT policy, but as of July 2024, it has yet to be finalized and published. GAO did not include HUD in its investigation or subsequent recommendations.
c. **Department of Justice**
    i. In criminal cases, there is no express legal requirement to disclose FRT use to the defense.
    ii. There is no comprehensive data available regarding the accuracy of the FRT that is used by law enforcement in its real-world application. For instance, there are no publicly available or standardized tests for the images used by law enforcement FRT systems for searches, such as low-resolution or grainy images from sources such as closed-circuit television (CCTV) cameras.
d. **Department of Homeland Security**
    i. CBP has implemented facial biometrics into the entry processes at all international airports and into the exit processes at 53 airports, as well as expanded facial biometrics at 40 seaports and all pedestrian lanes at the Southwest and Northern Border ports of entry.
    ii. TSA is using facial identification to verify a passenger's identity at security checkpoints using the CBP Traveler Verification Service (TVS), which creates a secure biometric template of a passenger's live facial image taken at the checkpoint and matches it against a gallery of templates of pre-staged photos that the passenger previously provided to the government (e.g., U.S. Passport or Visa).
    iii. In testimony to the Commission, GAO indicated that Homeland Security Investigations (HSI) was the only agency requiring staff to take FRT training prior to using services.
    iv. DHS, through its Science and Technology Directorate, funds FRT research, testing, and evaluation at the Maryland Test Facility (MdTF).
        1. MdTF is a first-of-its kind FRT testing center, and DHS is the only known federal department that funds and contracts with an FRT testing lab.

2. MdTF specializes in "scenario testing," which tests FRT use cases by simulating the full biometric system, testing how FRT performs in its intended use.

v. There are limited responsibilities that fall under DHS's Office of Civil Rights and Civil Liberties (CRCL). CRCL's role is to "minimize[e] bias in operational use, and safeguard [] individuals against disparate impacts based on protected characteristics."

vi. CRCL considers several broad themes when reviewing and supporting DHS's FRT programs, including discrimination, accuracy, scale, flexibility, use, perception, redress, unintended consequences, and validation.

e. **Department of Housing and Urban Development**

i. HUD is proliferating FRT use largely through its grant programs for public housing agencies (PHAs), putting FRT in the hands of grantees with no regulation or oversight.

ii. If HUD is providing funds for FRT—which is known to have higher misidentification rates for minorities—in housing where tenants are disproportionately female and people of color, issues relating to access, eviction, and other punishments could lead to Title VI violations.

iii. HUD does not require specific policies on FRT for PHAs and does not keep a list of PHAs that elect to use FRT.

iv. In April 2023, HUD issued a notice clarifying that ESSG funding can no longer be used to purchase FRT. However, this rule does not apply retroactively. There is no oversight mechanism in place to identify past instances where FRT was purchased with ESSG funding.

v. FRT raises significant privacy concerns among low-income tenants, as landlords and PHAs contract with AI companies to store residents' and their visitors' biometric data. The more entities have access to sensitive and identifying data, the more vulnerable they are to a data security breach.

vi. PHAs often cite public safety as the reason for FRT use, claiming that FRT is safer for building access because 1) keys can be lost or stolen, and 2) they can share surveillance footage with local law enforcement agencies to deter crime and identify perpetrators.

vii. There is no comprehensive data available regarding the purchasing of FRT by PHAs, and since HUD does not track or monitor FRT purchases via federal funds, it is difficult to determine how often these funds are being used for purposes of eviction.

IV. Accuracy & Bias in Testing:

a. National Institute of Standards and Technology **(**NIST) testing is voluntary; developers decide if they want to submit their algorithms for testing. Therefore, NIST testing reports provide a snapshot of a group of FRT programs at a given time, and in a laboratory rather than under real-world conditions. Thus, NIST cannot say that its

evaluated programs are accurately representative of the performance of all FRT deployed throughout the country.

b. Algorithmic accuracy rates can vary widely among developers and can result in false positive and false negative matches.
c. Even with the highest-performing algorithms, tests have shown there are likely to be false positives for certain demographic groups, specifically Black people, people of East Asian descent, women, and older adults.
d. One of the important factors in reducing bias appears to be the selection of data used to train algorithmic models. If algorithms are trained on data sets that contain very few examples of a particular demographic group, the resulting model will be worse at accurately recognizing members of that group in real-world deployments.
e. FRT human reviewers are not immune from "automation bias," or the propensity for humans to favor suggestions from automated decision-making systems and ignore, or fail to seek out, contradictory information made without automation.
f. While a human reviewer may be a useful safeguard against false matches, without specialized training, human reviewers make the wrong decisions about matches half the time.

V. **Transparency**

a. There is no comprehensive data available regarding the real-world accuracy of FRT as it is used by law enforcement.
b. There is no publicly available testing of the images used by law enforcement FRT systems.

Recommendations

I. **To Congress - Legislation**

a. Congress should direct and empower NIST to:
    i. Evaluate FRT algorithms sold to law enforcement
    ii. Report error rates disaggregated by demographic groups
    iii. Develop an operational testing protocol that agencies can use to assess how effective, equitable, and accurate their FRT systems are when actually deployed
    iv. Condition the receipt of federal funds by grantees on the adoption of national training standards for individuals who review and analyze the results returned by FRT algorithms (commonly referred to as "humans-in-the-loop") before those results are shared with investigators
    v. Require at least bi-annual testing of FRT systems as actually deployed (operational testing) to ensure low real-world error rates
        1. Results should be made publicly available in concise, clear, and accessible language to enable review by a nontechnical audience and with the context necessary to understand the relevance and any limitations of these assessments

2. This testing should be conducted either by independent, expert third-party testers (such as biometrics testing labs or qualified academic labs) or according to a legislatively approved testing protocol developed by independent experts

b. Provide a statutory mechanism for legal redress by individuals harmed by misuse or abuse of FRT. Legislation should include meaningful enforcement for statutory violations, such as civil damages for any person injured as a result of a violation.

II. To Chief AI Agency Officers – Testing & Training

a. Develop and incentivize the adoption of national training standards for individuals who review and analyze the results returned by FRT algorithms (commonly referred to as "humans-in-the-loop") before those results are shared with investigators.

b. Federal agencies should work with NIST to develop and implement field testing programs for their FRT systems.

c. For FRT that is rights-impacting:

i. Assess the AI in a real-world context to determine whether the FRT model results in significant disparities in the model's performance (e.g., accuracy, precision, reliability in predicting outcomes) across demographic groups.

ii. Mitigate disparities that lead to, or perpetuate, unlawful discrimination or harmful bias.

iii. Consult affected communities, including underserved communities, to solicit feedback, where appropriate, in the design, development, and use of FRT and use such feedback to inform agency decision-making regarding FRT.

d. Consult DHS' Maryland Test Facility as a template for the "Build Once, Use Widely" approach to real-world FRT testing to ensure the FRT will work in its intended real-world contexts.

III. To Departments Using FRT

a. **<u>Oversight</u>**

i. Agencies should post publicly on their websites whether the agency uses FRT, and whether training is required prior to such use.

ii. Ensure Chief AI Officers work in close coordination with existing responsible officials and organizations within their agencies, including Civil Rights and General Counsel offices, to advise and update agency FRT guidance, implementation, and oversight.

iii. Cultivate greater community trust by adopting more inclusive designs and engaging with communities to help individuals understand the technology's capabilities, limitations, and risks.

iv. Support research to improve accuracy and minimize demographic biases of current and potential FRT uses.

v. Agencies should audit their FRT use and ensure it complies with government policy.

b. **<u>Transparency</u>**

i. Any agency using FRT should have a publicly available use policy.

ii. In appropriate settings, provide clear and noticeable opt-out mechanisms to individuals whenever facial and biometric data is being collected, processed, or analyzed by FRT.
iii. Provide verified results with respect to accuracy and performance across demographics from NIST's Facial Recognition Technology Evaluation or a similar government-validated third-party test.
iv. FRT should be only part of a multi-factor basis for an arrest or investigation, in line with current fact-sensitive determinations of probable cause and reasonable suspicion.
v. Adopt policies to disclose to criminal suspects, their lawyers, and judges on a timely basis the role FRT played in law enforcement actions, such as lead identification, investigative detention, establishing probable cause, and arrest.
vi. Disclose to suspects and their lawyers, on arrest and in any subsequent charging document, that FRT was used as an element of the investigation that led to the arrest and specify which FRT product was used.
vii. Disclosure and consent requirements are insufficient in providing consumers agency over their data used in housing and financial services decisions; in addition to adequate privacy protections, consumers should be able to consent to how, where, when, and under what circumstances their personal data will be utilized.

c. **Procurement**
   i. Require that all FRT technology procured by the federal government meet NIST's minimum accuracy level.
   ii. FRT vendors should provide law enforcement agency users with ongoing training, technical support, and software updates needed to ensure their FRT systems can maintain high accuracy across demographic groups in real-world deployment contexts.

d. **Department of Justice**
   i. Update federal grant material in accordance with the recommendations described herein and publish on DOJ's public-facing website.
   ii. Conduct regular audits to determine if users complied with department policies when using FRT to conduct searches.
   iii. Police departments receiving federal grants and/or funding should establish guardrails for law enforcement's FRT use. These should include:
      1. Requirements that possible matches be used only as an investigative lead and not as the sole ground for probable cause
      2. Restricting use of FRT algorithms to those that have been evaluated by NIST and achieved a sufficiently high level of performance
      3. Assurance that all FRT tools used by an agency have a mechanism to allow agency command staff to readily review user search activity and detect misuse

e. **Department of Homeland Security**

i. Update federal grant material in accordance with the recommendations described herein and publish on DHS' public-facing website.

f. **Department of Housing and Urban Development**

i. Update federal grant material in accordance with the recommendations described herein and publish this information on HUD's public-facing website.

[This page is left intentionally blank]

Statement of Chair Garza

As a nation, we stand at a pivotal moment at the intersection of technological advances and individual privacy rights—where federal policy decisions will define the trajectory of our civil liberties in the age of Artificial Intelligence (AI). The most pressing of AI issues is the use of Facial Recognition Technology (FRT) by our federal government, the regulation of its use (or lack thereof), and balancing its use against the rights guaranteed by the U.S. Constitution.

It has been well documented that FRT has had a disproportionately negative impact on marginalized communities, particularly people of color—especially women. At the hearing, for example, we heard from AI Policy expert Bertam Lee about a black woman in Detroit who was misidentified by FRT and subsequently arrested, leading to early labor. As a mother of two, I find this concerning and agree with Office of Management and Budget's (OMB) assessment that federal agencies should not be allowed to use technology like FRT if they cannot prove measurable benefits that meaningfully outweigh the risks of use.[687] Moreover, the rules and regulations governing the use of AI lag significantly behind technological advancements. This gap leaves citizens vulnerable to abuses of power and bevy of privacy concerns. While FRT offers potential benefits, such as in the case when Clearview AI's photo database helped investigators identify a suspect in a child exploitation case—leading to his arrest, the discovery of thousands of illegal images, and the rescue of a 7-year-old girl, with the suspect now serving 35 years in prison—the rapid expansion of this technology without necessary safeguards poses serious risks to our civil liberties.[688]

Recognizing this emerging issue, the Commission unanimously voted to investigate the civil rights implications of the federal use of facial recognition technology. Our investigation focused on how FRT is developed and utilized by the U.S. Department of Justice (DOJ), the U.S. Department of Homeland Security (DHS), and the U.S. Department of Housing and Urban Development (HUD), as well as any safeguards being implemented to mitigate potential civil rights issues.

Impact at the Border

My roots run deep in the Rio Grande Valley, where my grandmother worked tirelessly to raise a large family with limited resources and opportunities. Her life, filled with struggle and sacrifice, instilled in our family a deep commitment to education and perseverance. Having worked as an immigration attorney and lifelong civil rights advocate, I am all too familiar with the challenges faced by people at the border, and I carry forward my grandmother's legacy in the ongoing fight for civil rights and equality—a fight that remains critical as we face new challenges in the digital age.

FRT has increasingly become a tool of surveillance at our nation's borders, often at the expense of migrants, immigrants, and communities of color.[689] The U.S. Department of Homeland Security

[687] Office of Management and Budget, "M-24-10: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," The White House, March 2024, available at https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf
[688] Report at 49
[689] Migration Policy Institute, "Artificial Intelligence at the Border: Shaping Privacy amid Security Concerns," available at https://www.migrationpolicy.org/article/artificial-intelligence-border-zones-privacy

(DHS) has been at the forefront of implementing this technology, yet the risks it poses are significant.[690] According to the National Institute of Standards and Technology (NIST), false positive rates in FRT are disproportionately higher for Black people, individuals of East Asian descent, women, and older adults.[691] At the border, a false positive could mean wrongful detainment or deportation—severe consequences for those already facing tremendous hardships. Moreover, the poor quality of images, especially for individuals from African and Caribbean nations, exacerbates these risks.[692] These are not just technical issues; they are reflections of systemic biases that have long plagued our nation's immigration and border policies.

Just after our briefing in March 2024, the Transportation Security Administration (TSA) announced a new requirement for migrants to submit to FRT to board domestic flights.[693] The TSA rule mandates that migrants without proper photo identification must have their identities verified through FRT, matching their information against DHS records. If a match cannot be made, migrants will be denied access to secure areas of the airport and prohibited from boarding their flights. Given the racially and ethnically diverse makeup of the U.S. immigrant population—9 percent identifying as Black, 20 percent as biracial, 27 percent as Asian, and 44 percent as Hispanic or Latino—the problem of false positives using FRT is especially troubling, as these inaccuracies can disproportionately affect these groups, leading to serious implications like wrongful detentions and barriers to accessing essential services.[694]

Impact on People of Color

The implications of FRT extend far beyond the border. Historically, technology has often been used to oppress rather than uplift marginalized communities by reinforcing systemic racism and bias. For instance, AI systems, which are frequently trained on data that lacks diversity, have been shown to perpetuate racial bias, disproportionately affecting Black, Asian, and Hispanic populations.

In the Commission's report, it is noted that "Arun Vemury of DHS S&T testified that through scenario testing, DHS has found that camera technologies can either fail to capture images, or capture lower quality images, for people with darker skin tones." During the Commission's site visit to the Maryland Test Facility (MdTF), Vemury further explained that while technology is continually advancing, and the best-performing systems—those combining high-performing algorithms and cameras—are expected to perform well across all demographic groups, DHS acknowledges a significant concern.[695] An FRT match might cognitively bias a reviewer's judgment of face similarity, reducing the likelihood of detecting a false positive.[696] Additionally, early research suggests that reviewers may become overly reliant on the technology, accepting its results without

[690] U.S. Department of Homeland Security, "Using AI to Secure the Homeland," available at https://www.dhs.gov/ai/using-ai-to-secure-the-homeland
[691] Report at 27
[692] Report at 61
[693] Valerie Gonzalez, "Migrants Lacking Passports Must Now Submit to Facial Recognition to Board Flights in U.S.," Associated Press, March 14, 2024, available at https://apnews.com/article/immigration-airport-security-facial-recognition-37b8f40ad768706cd335d9254e6a07e4#
[694] Migration Policy Institute, "Frequently Requested Statistics on Immigrants and Immigration in the United States, 2024," available at https://www.migrationpolicy.org/article/frequently-requested-statistics-immigrants-and-immigration-united-states-2024#characteristics; Report at 27
[695] U.S. Dep't of Homeland Security, Science & Technology Directorate, Site Visit Presentation at MdTF, Apr. 18, 2024.
[696] Vemury Statement, at 2-3

sufficient scrutiny, regardless of the accuracy.[697] The higher rates of false positives among people of color mean that these communities are more likely to be subjected to wrongful scrutiny and discrimination.

Additionally, the tech industry's mostly white workforce and leadership have led to the development of technologies that fail to address the needs of diverse communities, thereby deepening existing inequities. This discriminatory harm is evident in sectors like criminal justice, housing, and finance, where AI tools have been used in ways that exacerbate racial and economic disparities.

Conclusion

Perhaps most troubling is the pattern of deploying new technologies on marginalized groups before expanding them to the broader population. What begins at the border often does not stay there. The use of FRT on migrants and immigrants sets a dangerous precedent, normalizing surveillance and the infringement of civil liberties that can then be applied to all American citizens.

The Commission's findings highlight that even with the highest-performing algorithms, there remains a significant risk of false positives for specific demographic groups, including Black people, individuals of East Asian descent, women, and older adults. To address these concerns, Congress should establish a statutory mechanism for legal redress for individuals harmed by the misuse or abuse of FRT, with meaningful enforcement measures, including civil damages for those injured by violations. Additionally, federal agencies, in collaboration with NIST, should implement comprehensive field testing for their FRT systems, particularly for those impacting individual rights. This should include real-world assessments of the technology to identify and mitigate any disparities in performance across demographic groups, and active consultation with affected communities, including underserved populations, to ensure that their feedback informs the design, development, and use of FRT. These steps are crucial to safeguarding civil rights and ensuring that technological advancements do not perpetuate discrimination or harmful bias.

This report is a call to action. As we continue to navigate the complexities of implementing FRT, we must prioritize the protection of civil liberties for all individuals, regardless of their status or location. The Commission's report provides a roadmap for addressing these concerns.

[697] Vemury Statement, at 2-3

[This page is left intentionally blank]

Statement of Vice Chair Nourse

This report focuses on the widespread use of facial recognition technology by federal agencies. There is no question that this technology is being used on a widespread scale at our airports, at our borders, and elsewhere by the federal government. Civil rights advocates should understand that these technologies raise serious concerns. I commend Commissioner Mondaire Jones for his leadership on this report and its focus on technical flaws in facial recognition systems. Here, I focus on legal issues based on information obtained after the report was completed.

We know that facial recognition has resulted in several wrongful arrests at the state and local level. Harvey Eugene Murphy, Jr., Michael Oliver, Najeer Parks, Randal "Quaran" Reid, Alonzo Sawyer, Robert Williams, and Porcha Woodruff were all wrongly arrested due to misidentification by facial recognition software. They missed multiple days of work, spent their own money to prove their innocence, and were left to fight the government, against all odds. Almost all these individuals were Black.[698]

In my experience, working on criminal justice issues, Washington D.C. tends to think that all problems live in Washington D.C. Criminal justice is a matter of state and local law. *So, while this report does yeoman service on the federal front, it should not be misread as focusing on two percent of the potential arrest population in the United States*. In 2019, there were over *ten million arrests* by state and local police;[699] by contrast, there were approximately 200,000 arrests by federal agencies, making the federal government responsible for two percent of all national arrests.[700]

While the FBI already recognizes that this technology cannot be used to establish the necessary constitutional requirements for a lawful arrest, as arrest statistics show, the FBI—and all federal agencies—are a very small part of the problem. I call on civil society organizations, state and local legislators, attorney generals, the Justice Department, and the COPs office (which spends federal money to support local police) to work diligently to ensure that *states and localities* get this message sooner rather than later, before more innocent individuals are wrongly arrested.

Wrongful arrests

No one disputes that facial recognition technology has led to wrongful arrests. Few dispute that it should never be the sole factor in charging or arresting an individual, nor should it constitute probable cause to arrest. I commend the Department of Justice's policy that limits the use of FRT for

---

[698] Nathan Freed Wessler, *Police Say a Simple Warning Will Prevent Face Recognition Wrongful Arrests. That's Just Not True.*, ACLU (Apr. 30, 2024), https://www.aclu.org/news/privacy-technology/police-say-a-simple-warning-will-prevent-face-recognition-wrongful-arrests-thats-just-not-true#:~:text=To%20date%2C%20there%20have%20been,person%20wrongfully%20arrested%20was%20Black.

[699] Uniform Crime Report, Crime in the United States, 2019, U.S. Department of Justice—Federal Bureau of Investigation (Fall 2020), https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/topic-pages/persons-arrested.pdf

[700] Federal Justice Statistics, 2019, Bureau of Justice Statistics (Oct. 2021), https://bjs.ojp.gov/library/publications/federal-justice-statistics-2019#:~:text=During%20fiscal%20year%20%28FY%29%202019%2C%20federal%20law%20enforcement,increase%20from%20the%20181%2C726%20arrests%20in%20FY%202009.

investigative leads only. However, our panelists highlighted that there is no way of confirming adherence to this rule in practice in the federal government or in the much, much vaster realm of state and local law enforcement.[701] And there are reasons to worry, as I explain below about a gap between such guidance and actual implementation.

Seven known wrongful arrests may seem like an exceedingly small number. But, as the report indicates, there are reasons why we may never know the true extent of the problem. If police do not voluntarily disclose the use of facial recognition technology, and are not forced to disclose its use, there may be no way to know. Given the *millions of people arrested* every year in the United States, we must worry that the seven incidents, known as I write, may be a very small part of the problem. Given the lack of information, we must also focus on *preventing wrongful arrests before they happen* by ensuring that state and local police have the proper instruction on when and how to use this technology.

State and local police should have an incentive to deploy this technology wisely. *They are subject to legal liability for wrongful arrests due to misuse of facial recognition.* The Detroit Police department knows this well. It thought it had a good facial recognition policy, but it did not prevent a wrongful arrest. In 2020, Robert Williams was wrongly arrested in front of his family due to facial recognition use. Williams brought suit, with the help of the American Civil Liberties Union. As part of the settlement, Detroit agreed to a set of practices for the use of facial recognition. The settlement, which is attached to this statement in Appendix A, does a good job of outlining specific steps that law enforcement should take to minimize wrongful arrest before it happens.

Notice that these policies are quite specific, and *specificity is important here.* Detroit had a policy that said, as does the FBI, that facial recognition should only be used for investigative leads. But, in practice, *such general statements were not enough* to protect against the wrongful arrests and identification of Robert Williams.

- A lineup identification procedure (such as a photographic lineup) may never be conducted based solely on a facial recognition investigative lead without the investigating officer first obtaining independent and reliable evidence linking a suspect to a crime. *See* DPD Directive No. 203.11, § 4.2(3), attachment C to the Settlement Agreement.

- A facial recognition lead, combined with a lineup identification, may never be a sufficient basis for seeking an arrest warrant. Before seeking an arrest warrant, a detective must document their independent investigative steps establishing probable cause (other than the

[701] Clare Garvie, Fourth Amendment Center Training and Resource Counsel, National Association of Criminal Defense Lawyers (NACDL), Testimony, *Civil Rights Implications of the Federal Use of Facial Recognition Technology Briefing Before the U.S. Comm'n on Civil Rights, Washington, DC* (Mar. 8, 2024).

FRT lead and any lineup procedure) and obtain sign-off from supervisory officials. *See* DPD Directive No. 307.5, § 5.3.[702]

- When requesting and conducting a facial recognition search, investigators and analysts must complete forms that document critical information about the FRT search—including the quality of the input photo and the size of the candidate list. *See* DPD Directive No. 307.5, § 5.5.

- Lineups may not incorporate the same photograph of a possible suspect that facial recognition identified as an investigative lead, to avoid the possibility that the original facial recognition "hit" is tainted. *See* DPD Directive No. 203.11, § 4.2(4).

- Witnesses performing lineup identifications may not be told that facial recognition identified anyone as an investigative lead. *See* DPD Directive No. 203.11, § 4.2(16).

- Police must provide documentation to the prosecutor if facial recognition has been used so that this information is available to defense counsel in discovery as potentially material or exculpatory information. *See* DPD Directive No. 307.5, § 5.5.

- Department officers cannot use facial recognition, unless they are trained on the risks and dangers of the technology, including that it misidentifies people of color at higher rates. *See* DPD Directive No. 307.5, § 5.4.

Federal government assistance

Now that we have seen the arrest problem at the state level, what can the federal government do? The federal government can assist states by establishing national standards and protocols for facial recognition use by state law enforcement. This effort should involve collaboration with stakeholder organizations and police officer associations to develop these policies. A national standard can help prevent wrongful arrests by addressing improper FRT procurement and use from the outset, if it is widely published.

In the meantime, it is important that our report and recommendations reach the state-level authorities, civil society, and law enforcement organizations to prevent further wrongful arrests of the innocent. For a start, the Justice Department should issue more specific guidelines when dispensing existing law enforcement funds to state and local entities when purchasing facial recognition technology.

When applying for funding for federal recognition, the Department of Justice's Assistance Grant (JAG) Program requires that grant recipients:

[702] These protections are intended to address the problem that facial recognition matches can taint subsequent witness identifications because the false matches are generated by an algorithm designed to output a candidate list of individuals appearing highly similar to the suspect.

> must have policies and procedures in place to ensure that the facial recognition will be used in an appropriate and responsible manner that promotes public safety; and protects privacy, civil rights, and civil liberties; and complies with all applicable provisions of the U.S. Constitution, including the fourth amendment's protection against unreasonable searches and seizures, the first amendment's freedom of association and speech, and other laws and regulations. Recipients utilizing funds for FRT must make such policies and procedures available to DOJ upon request.[703]

That guidance allows for a vast amount of leeway, so the Department must issue more specific guidelines, along the lines noted above. Local police departments receiving DOJ grant money should verify that recipients are not using these funds to purchase and use facial recognition software that could result in discrimination prohibited by Title VI.

In sum, the Department of Justice can play a very important role in preventing wrongful arrests by creating specific bias-reduction policies. It controls billions of dollars every year that provide federal funding for state and local police. Its investigative arms, like the National Institute of Justice, the Civil Rights Division, and the policy arms of the Department should provide the expertise necessary to help state and local police prevent wrongful arrests. Given that the wrongful arrests we know have disproportionately affected Black citizens, it is imperative that the Department take a leadership role in creating *specific guidelines*. It is not enough to gesture to "civil rights" protections or to say that facial recognition should only be used for investigative leads. To the extent the report offers findings and recommendations to support this mission, I heartily concur.

[703] Bureau of Justice Assistance, "Bureau of Justice Assistance Edward Byrne Memorial Justice Assistance Grant (JAG) Program Frequently Asked Questions (FAQs)" (May 2024), https://bja.ojp.gov/doc/jag-faqs.pdf.

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

ROBERT JULIAN-BORCHAK WILLIAMS,

Plaintiff,

v.

CITY OF DETROIT, a municipal corporation, DETROIT POLICE CHIEF JAMES WHITE, in his official capacity, and DETECTIVE DONALD BUSSA, in his individual capacity,

Defendants.
_____/

Case No. 21-10827

Hon. Laurie J. Michelson
Mag. Judge David R. Grand

STIPULATED ORDER OF VOLUNTARY DISMISSAL WITH PREJUDICE

The parties, through their respective counsel, hereby stipulate and agree as follows:

1. Plaintiff and Defendants have reached a negotiated resolution in this matter. To that end, the parties have entered into a Settlement Agreement. *See* Exhibit 1 and the attachments thereto.
2. Pursuant to the stipulation of the parties and Fed. R. Civ. P. 41(a), and consistent with the above, all of Plaintiff's claims in this lawsuit against all Defendants are dismissed with prejudice and without costs.

3. The Court hereby retains jurisdiction to enforce the Settlement Agreement for four years from the date of the entry of this order.

IT IS SO ORDERED.

Dated: June 28, 2024

s/Laurie J. Michelson
LAURIE J. MICHELSON
UNITED STATES DISTRICT JUDGE

The parties stipulate to the entry of the above order:

/s/Michael J. Steinberg
Michael J. Steinberg (P43085)
Julia Kahn*
Nethra Raman*
Collin Christner*
Ewurama Appiagyei-Dankah*
Civil Rights Litigation Initiative
University of Michigan Law School
701 S. State St., Suite 2020
Ann Arbor, MI 48109
(734) 763-1983
mjsteinb@umich.edu
jekahn@umich.edu
nethra@umich.edu
collindc@umich.edu
eadankah@umich.edu

Philip Mayor (P81691)
Daniel S. Korobkin (P72842)
Ramis J. Wadood (P85791)
American Civil Liberties Union Fund of Michigan
2966 Woodward Ave.
Detroit, MI 48201
(313) 578-6803
pmayor@aclumich.org
dkorobkin@aclumich.org
rwadood@aclumich.org

Nathan Freed Wessler
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, New York 10004
(212) 549-2500
nwessler@aclu.org

Counsel for Plaintiff

*Student Attorney practicing pursuant to Local Rule 83.21

/s/ Patrick M. Cunningham
Patrick M. Cunningham (P67643)
City of Detroit Law Department
2 Woodward Avenue, Suite 500
Detroit, MI 48226
(313) 237-5032
cunninghamp@detroitmi.gov

Counsel for Defendants

Dated: 6/25/24

EXHIBIT 1

Settlement Agreement with Attachments A-E

SETTLEMENT AGREEMENT
WILLIAMS v. CITY OF DETROIT, et al.,
EASTERN DISTRICT OF MICHIGAN CASE NUMBER: 21-cv-10827

1. Preamble. The City of Detroit and Chief James White ("Defendants") recognize the need to safeguard the Fourth Amendment rights of individuals involved in a criminal investigation and to ensure that policy advances to keep pace with evolving technology used to fight crime in the City of Detroit, and therefore hereby enter into this settlement agreement with Plaintiff Robert Julian-Borchak Williams ("Plaintiff").

2. Purpose. Defendants and Plaintiff (collectively the "Parties") intend for this Agreement to settle and resolve the dispute referenced above, *Williams v. City of Detroit, et al.*, case number 21-cv-10827, filed in the United States District Court for the Eastern District of Michigan ("the Court"). This Agreement represents the compromise of a disputed claim and is not to be construed as an admission of liability on the part of Defendants.

3. Facial Recognition Manual Directive. Defendants agree to implement and enforce the attached Detroit Police Department ("DPD") Manual Directive 307.5 ("Facial Recognition"), which was approved by the Detroit Board of Police Commissioners (the "BOPC") on May 30, 2024. *See Attachment A*.

4. Facial Recognition Forms. Defendants agree to implement and instruct DPD personnel to use the attached investigative lead report and vetting

report forms. *See Attachment B*. DPD policy shall require that the relevant portions of these forms be completed by DPD Crime Intelligence Unit examiners and DPD investigators in connection with any facial recognition search.

5. Eyewitness Identification and Lineup Manual Directive. Defendants agree to implement and enforce the provisions of the attached DPD Manual Directive 203.11 ("Eyewitness Identification and Lineups") that have been added or changed between the date this lawsuit was filed on April 13, 2021, and the effective date of this Agreement, which was approved by the BOPC on May 30, 2024. *See Attachment C*.

6. Audit of Prior Cases. Within 180 days of the execution of this agreement, the DPD's Civil Rights Division will conduct an audit of all cases in which facial recognition technology was utilized to generate an investigative lead that was followed by an arrest or the issuance of an arrest warrant. The audit will be based upon a log of facial recognition requests maintained by DPD's Crime Intelligence Unit beginning on February 22, 2017. The audit will examine qualifying arrests made and arrest warrants issued through August 10, 2023. Auditors will identify all cases in which an arrest was made or a warrant was issued after an investigative lead was generated, and then determine: whether a live or photo lineup was utilized; whether there was an independent basis for the arrest such as an outstanding warrant or probable cause that the individual committed a

separate arrestable offense at another time or place; whether there was independent evidence supporting the arrest or issuance of the arrest warrant, and identify such independent supporting evidence in a written audit log. In the event that the audit reveals arrests made or arrest warrants issued following an investigative lead alone or an investigative lead and lineup identification that are unsupported by independent evidence, the DPD will notify the appropriate prosecutor. Active investigations subject to this audit shall comply with Manual Directives 203.11 and 307.5 prior to an arrest or the issuance of an arrest warrant.

7. Training Program. Defendants agree that DPD shall implement and abide by the attached Training Program for DPD for four years from the effective date of this agreement. *See Attachment D*.

8. Future Modifications to Manual Directives. Defendants may seek approval of future modifications of DPD Manual Directives 307.5 or 203.11 from the BOPC. However, Defendants agree that for four years following the effective date of this agreement, they shall not propose or make any substantive modifications that reduce, decrease, or remove protections in either policy that were added or changed between the filing of this lawsuit on April 13, 2021, and the effective date of this Agreement. This limitation on substantive modifications includes, but is not limited to any potential modification that would, (1) authorize investigators to conduct a lineup based on a facial recognition investigative lead

without first developing an independent and reliable basis for conducting the lineup, or to request an arrest warrant based only upon such a lineup combined with a facial recognition-derived investigative lead; (2) eliminate or reduce the number of supervisory officers who must approve investigative actions or arrest warrant requests made pursuant to either policy; (3) authorize photographic lineups to be conducted, (a) with a non-eyewitness, (b) in a non-blind fashion, (c) in a non-consecutive manner, or (d) containing a photograph derived from a facial recognition technology search; or (4) authorize DPD members to inform a witness to be administered a photographic lineup that facial recognition has been used to generate an investigative lead. When proposing any modifications of either policy to the BOPC, Defendants shall provide the proposed modifications to the ACLU Fund of Michigan.

9. Release of Claims for Damages, Attorneys' Fees, and Costs. The Parties agree that Plaintiff's claims for damages, attorney fees, and costs have been resolved as described in the attached General Release. See *Attachment E*. The Parties agree that Attachment E will be redacted in its entirety when this Agreement is filed with the court.

10. Breach of Terms. A breach of any term of this Agreement may be enforced by any party by filing a motion before the Court for enforcement of the Agreement. The party establishing a breach of this Agreement may be entitled to

equitable relief, costs, or attorney fees authorized by law, as determined by the Court.

11. Entry of Stipulated Order of Dismissal. Contemporaneous with the Parties' execution of this Agreement, the Parties through their counsel stipulate to the entry of an order of dismissal with prejudice ("Stipulated Order"), attached to which as an exhibit shall be an executed copy of this Agreement. The Stipulated Order shall expressly retain the Court's jurisdiction to enforce this Agreement for four years following the date of the Stipulated Order. In the event that the Court refuses to enter the Stipulated Order or retain jurisdiction to enforce this Agreement, this Agreement shall be null and void unless the Parties are able to agree to alternative terms.

12. Effective Date. This Agreement shall become effective immediately upon the Court entering the Stipulated Order.

13. Execution. This Agreement may be executed in counterparts, and is fully executed on the date by which both Parties have executed this agreement. Facsimiles and PDF versions of signatures will constitute acceptable, binding signatures for purposes of this Agreement.

14. Severability. If any provision of this Agreement, or part thereof, is held invalid, void, or voidable as against public policy or otherwise, the invalidity shall not affect other provisions, or parts thereof, which may be given effect

without the invalid provision or part. To this extent, the provisions, and parts thereof, of this Agreement are declared to be severable.

15. Entire Agreement. This Agreement and the attachments thereto contain all the terms and conditions agreed upon by and between the Parties. Other than the attachments to this Agreement, no oral agreement between Plaintiff and Defendants entered into at any time, nor any written agreement between Plaintiff and Defendants entered into prior to the execution of this Agreement regarding the subject matter of the instant proceeding, shall be deemed to have any force or effect, or to bind the Parties hereto, or to vary the terms and conditions contained herein.

Conrad L. Mallett, Jr. (P30806)
Corporation Counsel
City of Detroit Law Department

Date: June 24, 2024

Patrick M. Cunningham (P67643)
Attorney for Defendants
City of Detroit Law Department

Date: June 24, 2024

Michael J. Steinberg (P43085)
Julia Kahn*
Nethra Raman*
Collin Christner*
Ewurama Appiagyei-Dankah*
Civil Rights Litigation Initiative

Date: June 25, 2024

University of Michigan Law School
701 S. State St., Suite 2020
Ann Arbor, MI 48109
(734) 763-1983
mjsteinb@umich.edu
jekahn@umich.edu
nethra@umich.edu
collindc@umich.edu
eadankah@umich.edu

Philip Mayor (P81691)
Daniel S. Korobkin (P72842)
Ramis J. Wadood (P85791)
ACLU Fund of Michigan
Attorneys for Plaintiff
2966 Woodward Ave.
Detroit, MI 48201
(313) 578-6803
pmayor@aclumich.org
dkorobkin@aclumich.org
rwadood@aclumich.org

Nathan Freed Wessler
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, New York 10004
(212) 549-2500
nwessler@aclu.org

*Student Attorney practicing pursuant to Local Rule 83.21

Attachment A

Revised Manual Directive 307.5
Regarding Facial Recognition

DETROIT POLICE DEPARTMENT MANUAL

Series	Effective Date	Review Date	Directive Number
300 Support Services		Annually	307.5
Chapter 307 – Information System			
Reviewing Office Crime Intelligence			☐ New Directive ☐ Revised
References:			

FACIAL RECOGNITION

307.5 - 1 PURPOSE

The purpose of this policy is to establish acceptable use *of Facial Recognition technology by* the Detroit Police Department (DPD). Facial Recognition shall only be used when there is reasonable suspicion that such use will provide information relevant to an active or ongoing *investigation of a* Part 1 Violent Crime or a first-degree Home Invasion. If *an investigative lead* is *developed* through DPD's *F*acial *R*ecognition *program*, it shall be considered *only* an investigative lead *that shall not be the sole ground for arrest or to apply for an arrest warrant*.

307.5 - 2 Definitions

307.5 - 2.1 Biometric Data

Data derived from one or more intrinsic physical or behavioral traits of humans, to include fingerprints, palm prints, iris scans, and *F*acial *R*ecognition data.

307.5 - 2.2 Examiner

An individual who has received advanced training in the *F*acial *R*ecognition *program* and its features. Examiners have at least a working knowledge of the limitations of *F*acial *R*ecognition. *Examiners are* qualified to assess image quality and appropriateness for *F*acial *R*ecognition searches and to perform one-to-many and one-to-one facial image comparisons.

307.5 - 2.3 Facial Recognition (FR)

The automated searching of a facial image in a biometric database (one-to-many), typically resulting in a group of facial images ranked by computer-evaluated similarity. All Facial Recognition searches must be corroborated by at least two examiners and one supervisor.

307.5 - 2.4 *First-degree Home Invasion*
A person who breaks and enters a dwelling with intent to commit a felony, larceny, or assault in the dwelling, a person who enters a dwelling without permission with intent to commit a felony, larceny, or assault in the dwelling, or a person who breaks and enters a dwelling or enters a dwelling without permission and, at any time while he or she is entering, present in, or exiting the dwelling, commits a felony, larceny, or assault is guilty of home invasion in the first degree if at any time while the person is entering, present in, or exiting the dwelling either of the following circumstances exists:
(a) The person is armed with a dangerous weapon.
(b) Another person is lawfully present in the dwelling. (MCL 750.110a(2)).

307.5 - 2.5 Part 1 Violent Crimes
For the purposes of this directive, Part 1 Violent Crimes are defined as robbery, sexual assault, aggravated assault, or homicide.

307.5 - 2.6 *Predictive Analysis*
The process of using data to forecast future outcomes.

307.5 - 2.7 Reasonable Suspicion
The specific facts and reasonable inferences drawn from those facts to convince an ordinarily prudent person that criminality is at hand.

307.5 - 2.8 Statewide Network of Agency Photos (SNAP)
A computer application managed by the SNAP Unit, deployed through the MiCJIN portal, which serves as an investigative tool and a central repository of images from local, state, and federal agencies.

307.5 - 3 Prohibited Uses

307.5 - 3.1 Surveillance
Members shall not use *F*acial *R*ecognition to surveil the public through any camera or video device.

307.5 - 3.2 Live Streaming or Recorded Videos
Members shall not use *F*acial *R*ecognition on live stream or on recorded videos. This prohibition applies to all videos, whether they originate from DPD itself, from private citizens, or from any other source.

307.5 - 3.3 Mobile Facial Recognition
Members shall not use mobile *F*acial *R*ecognition.

307.5 - 3.4 Predictive Analysis
Members shall not use *F*acial *R*ecognition for predictive analysis.

307.5 - 3.5 First Amendment Events
The Detroit Police Department will not violate First, Fourth, and Fourteenth Amendments and will not perform or request *F*acial *R*ecognition searches about individuals or organizations based solely on the following:

a. Their religious, political, or social views or activities;
b. Their participation in a particular noncriminal organization or lawful event; or
c. Their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law.

307.5 - 3.6 Facial Recognition Use for Immigration Enforcement
DPD members are strictly prohibited from using *F*acial *R*ecognition to assess immigration status.

307.5 - 4 Discipline

1. Any violations to this policy shall be deemed major misconduct. Any misuse of the *F*acial *R*ecognition *program* will be investigated and reviewed for criminality. The remedy for this misconduct is dismissal from DPD.

2. If *F*acial *R*ecognition is used contrary to section 307.5 -3.5 First Amendment Events, DPD shall notify the Board of Policy Commissioners, the Mayor of Detroit, City Council President, and City Council President Pro Tem within 24 hours of the violation.

307.5 - 5 Use of Facial Recognition Technology

307.5 - 5.1 Use Limited to Still Images
F*a*cial *R*ecognition *technology* may only be used on a still image of an individual, *including still images captured from video.*

307.5 - 5.2 Criminal Investigation Required
Members shall not use *F*acial *R*ecognition technology unless *there is reasonable suspicion that use of Facial Recognition technology will provide information relevant to* an active or ongoing *investigation of a* Part 1 Violent Crime or a *first-degree* Home Invasion.

307.5 - 5.3 *An Arrest or Arrest Warrant Request Following Use of Facial Recognition Technology Must Be Supported by Additional Independent Reliable Evidence*
Probable cause must be established for an arrest or for an arrest warrant request must be established using legally authorized methods other than Facial Recognition. Examples of other investigative methods may include, but are not limited to cellular data analysis; eyewitness testimony, establishment of a timeline, DNA, etc. A request for an arrest warrant, or an arrest, shall not be made solely on the basis of an investigative lead developed through Facial Recognition technology in combination with a lineup identification. A request for an arrest warrant, or an arrest, must be supported by additional independent reliable evidence.

307.5 Facial Recognition

307.5 - 5.4 Process for Requesting Facial Recognition

1. Requests for Facial Recognition services shall be submitted to the Crime Intelligence Unit (CIU), with photograph(s) to be reviewed, the incident number, the crime type, and other pertinent information.

   a. *Members requesting Facial Recognition services shall affirm that they have completed investigative Facial Recognition training;*

   b. *Members performing Facial Recognition services shall confirm that the requesting member has made the affirmation above.*

307.5 - 5.5 *Process for Performing Facial Recognition*

1. *Prior to the use of Facial Recognition, a CIU examiner shall complete the Real Time Crime Center – Facial Recognition Vetting form, which shall contain:*
   a. *The requestor's name, rank, and command;*
   b. *Confirmation that the requestor has affirmed that they have completed investigative Facial Recognition training;*
   c. *The crime being investigated (Part 1 Violent Crime or first-degree Home Invasion);*
   d. *The role the individual in the probe image is reasonably suspected to have played in the incident; and*
   e. *A description of the probe image quality.*

2. *CIU shall reject a request for Facial Recognition when:*
   a. *The request fails to identify the requestor's name, rank or command;*
   b. *The requestor fails to affirm that they have completed investigative Facial Recognition training;*
   c. *The crime being investigated is not a Part 1 Violent Crime or first-degree Home Invasion;*
   d. *There is not a reasonable suspicion that the individual in the probe image had a role in the commission of the crime; or*
   e. *The quality of the probe image is unsuitable for Facial Recognition.*

3. CIU shall perform Facial Recognition searches utilizing SNAP, which includes criminal mug shot images. In the event additional analysis is needed for confirmation of an investigative lead, a formal request may be made to MSP to search the state's database. Any such request must be approved by a CIU supervisor.

4. If the examiner *develops* an investigative lead, the examiner must corroborate this lead with at least one other examiner and a CIU supervisor. *Both examiners and the CIU supervisor shall sign off on the investigative lead.*

5. Upon final approval, CIU shall complete *an investigative lead* report for the requestor. *This investigative lead report must be attached to any request for a warrant for any person named in the investigative lead report.* The investigative lead report shall include the following language:

307.5 Facial Recognition

- "The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any *possible* connection or involvement of any subject to the investigation must be determined through further *independent* investigation and investigative resources."

- *"Facial Recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the probe image's quality, lighting, face angle, and face obstructions, among other factors."*

- *"Facial Recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).*

In addition, the investigative lead or vetting report shall also:

- *Disclose the probe image used to run the Facial Recognition search (in both its original form and with any enhancements), and identify all features of the probe image that may reduce the reliability of the Facial Recognition result (such as low light, low pixel density, angle of face, partial occlusion of face, etc.), and any enhancements or modifications made to the probe image during the course of the search process;*

- *Disclose each of the following: the date the investigative lead image was taken, how many other images of the same individual in the investigative lead image exist in the database that was searched, and, if other images of the same individual exist in the database, the dates when each was taken.*

6. *In any case in which charges are filed and in which Facial Recognition technology was used at any stage of the investigation, the member responsible for that investigation shall provide the following to the Wayne County Prosecutor's Office (WCPO):*

    - *Any investigative lead report and vetting report;*

7. In the event that *an investigative lead* cannot be developed, the requestor will be notified that no *investigative lead was developed.*

307.5- 5.6 Outside Agency Using Facial Recognition

An outside agency, or investigators from an outside agency, may request *Facial Recognition* searches *by DPD* to assist with investigations only if the following requirements are met:

a. Prior to making the request, the outside agency has a formalized agreement (e.g. a memorandum of understanding or an interagency agreement) between *DPD* and the outsideagency;
b. The outside agency is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in this directive and the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number) and acknowledges an agreement with the following statement:

   - "The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any *possible* connection or involvement of any subject to the investigation must be determined through further *independent* investigation and investigative resources."

c. If any agency is found not in compliance with this Directive, *DPD* shall immediately suspend all Facial Recognition requests until the requesting agency becomes in compliance with this Directive.

307.5 - 6 Governance and Oversight

307.5 - 6.1 LASO & *CIU* Responsibilities

1. The primary responsibility for the operation of *DPD*'s criminal justice information systems, *F*acial *R*ecognition program and system, operations, and the coordination of personnel, the receiving, seeking, retention, evaluation, data quality, use, purging, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the Local Agency Security Officer (LASO) who is assigned to Technical Services.

2. The LASO will be responsible for the following:

   a. Overseeing and administering the *F*acial *R*ecognition program to ensure compliance with applicable laws, regulations, standards, and policy;
   b. Acting as the authorizing official for individual access to *F*acial *R*ecognition information;
   c. Ensuring that user accounts and authorities granted to personnel are maintained in a current and secure "need-to-know" status; and
   d. Ensuring that random evaluations of user compliance with system requirements along with this policy and applicable laws are conducted and documented;

3. The commanding officer of *CIU* will be responsible for the following:

   a. Reviewing *F*acial *R*ecognition search requests, reviewing the results of *F*acial *R*ecognition searches, and returning the most likely candidates – or candidate images – if any, to the requestor.
   b. Ensuring and documenting that personnel (including investigators from external agencies who request *F*acial *R*ecognition searches) meet all prerequisites stated in this policy prior to being authorized to use the *F*acial *R*ecognition system.

4. *Members of investigative entities shall be responsible for the following:*

   a. *In the event that the Facial Recognition program develops an investigative lead, prior to making any probable cause arrest, or requesting a warrant from the (WCPO), the member must obtain written approval from their commanding officer and the commanding officer of Investigative Operations.*

5. *DPD* is guided by applicable laws, regulations, and standards to ensure that privacy, civil rights, and civil liberties are not violated by this Facial Recognition policy or by the *DPD*'s *F*acial *R*ecognition information collection, receipt, access, use, dissemination, retention, and procedure.

307.5 - 6.2 Weekly Report to the Board of Police Commissioners

DPD shall provide a weekly report to the Board of Police Commissioners with information pertaining to the number of *F*acial *R*ecognition requests that were fulfilled, the crimes that the *F*acial *R*ecognition requests were attempting to solve, the number of leads developed from the *F*acial *R*ecognition *program, and the number of searches that did not produce investigative leads.* During this report, if there are any upgrades to the Facial Recognition software, any planned changes to the contract, and/or any confirmed policy violations, *DPD* shall notify the Board of Police Commissioners.

307.5 – 6.3 Annual Report to the Board of Police Commissioners

DPD shall provide an annual report to the Board of Police Commissioners. This annual report shall include a summary of the weekly reports and an evaluation of the efficacy of the *DPD*'s *F*acial *R*ecognition technology. The evaluation shall include any relevant lawsuits or settlements involving *F*acial *R*ecognition, the number of cases *in which* use of the technology assisted in investigations, and any other relevant factors. This shall be disseminated at the Board of Police Commissioners' meeting, and electronic copy shall be provided to the Board for dissemination to the public.

307.5 - 6.4 All Policy Changes to the Board of Police Commissioners
DPD shall seek the Board of Police Commissioners' approval regarding any and all changes to *this manual directive*.

307.5 - 7 Security and Maintenance

1. *DPD* will comply with generally accepted industry or other applicable standards for security to protect data at rest, in motion, or in use. Security safeguards will cover any type of medium (printed or electronic) or technology (e.g. physical servers, virtual machines, and mobile devices) used in a work-related *DPD* activity. *DPD*'s *F*acial *R*ecognition system will operate in a secure facility protected with multiple layers of physical security from external intrusion and will utilize secure internal and external security and privacy safeguards against network intrusions, such as strong multifactor authentication; encrypted communications; firewalls; and other reasonable physical technological, administrative, procedural, and personnel security measures to minimize the risks of unauthorized access to the system.

   Access to the *DPD*'s *F*acial *R*ecognition information from outside the facility will be allowed only over secure networks. All results produced by *DPD* as a result of a *F*acial *R*ecognition search are disseminated by secured electronic means (such as an official government e-mail address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee. When such non-electronic dissemination is made, the member shall memorialize the dissemination as follows:

   a. To whom it was released;
   b. Date and time it was released; and
   c. Manner in which it was released (i.e. if by phone, include the number; if in person, include name of witness who saw it released).

2. All members with access to *DPD*'s information or information systems will report a suspected or confirmed breach to their immediate supervisor who will ensure that the LASO) is notified as soon as possible without unreasonable delay, consistent with applicable laws, regulations, policies, and procedures. This includes a breach in any medium or form, including paper, oral, *or* electric. Following assessment of the suspected or confirmed breach and as soon as practicable, *DPD* will notify the originating agency from which the entity received *F*acial *R*ecognition information of the nature and scope of a suspected or confirmed breach of such information. *DPD* will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.

3. All *F*acial *R*ecognition equipment and *F*acial *R*ecognition software and components will be properly maintained in accordance with the manufacturer's recommendations, including routine updates as appropriate.

307.5 Facial Recognition

4. *DPD* will store *F*acial *R*ecognition information in a manner that ensures that it cannot be modified, accessed, or purged except by members authorized to take such actions.

5. Authorized access to the *DPD*'s *F*acial *R*ecognition system will be granted only to members whose positions and job duties require such access and who have successfully completed a background check and required training.

6. Usernames and passwords to the *F*acial *R*ecognition system are not transferrable, must not be shared by *DPD* members, and must be kept confidential.

7. The system administrator (LASO) will ensure that all manufacturer- generated default passwords are replaced with secure passwords before web-based interfacial of the system become operational. User passwords must meet the standards outlined in Manual Directive 307.4, Criminal Justice Information Systems (CJIS).

8. Queries made to *DPD*'s *F*acial *R*ecognition system will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.

9. *DPD* will maintain an audit trail of requested, accessed, searched, or disseminated *F*acial *R*ecognition information. An audit trail will be kept for a minimum of one (1) year of requests, access, and searches of *F*acial *R*ecognition information for specific purposes and of what *F*acial *R*ecognition information is disseminated to each individual in response to the request. Audit logs will include:

   a. The name and unit of the law enforcement user;
   b. The date of access;
   c. Case number; and
   d. The authorized law enforcement or public safety justification for access including a relevant case number.

Attachment B

Investigative Lead Report and Vetting Report Forms

The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and **IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT.** Any possible connection or involvement of any subject to the investigation must be determined through further independent investigation and investigative resources.

Facial recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the input image's quality, lighting, face angle, and face obstructions, among other factors.

Facial recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).

REAL TIME CRIME CENTER — FACIAL RECOGNITION INVESTIGATIVE LEAD

The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and **IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT**. Any possible connection or involvement of any subject to the investigation must be determined through further independent investigation and investigative resources. Facial recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the input image's quality, lighting, face angle, and face obstructions, among other factors. Facial recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).

REQUEST #:	23-00						
REQUEST DATE/TIME:							
REPORT NUMBER:							
CRIME:	☐Homicide ☒Robbery/Carjacking ☐Aggravated Assault/NFS ☐CSC 1/CSC 3 ☐Home Invasion 1						
REQUESTER NAME:		**RANK:**	Choose an item	**COMMAND:**			
REASON:	☒ Reasonable Suspicion of a Part I Violent Crime or First-Degree Home Invasion ☐ Physical Incapacity/Mental Incapacity/At-Risk Person/Deceased Person (Homicide Only)						
IMAGES:	**ORIGINAL IMAGE**		**INQUIRY IMAGE**		**INVESTIGATIVE LEAD**		
IMAGE SOURCE:	Choose an item		Choose an item.		SNAP	**Date**	
IMAGE ENHANCEMENTS:	Choose an item		Choose an item.		None		
# OF IMAGES PRODUCED IN GALLERY:		**# OF LEAD IMAGES IN DATABASE:**		**DATES OF LEAD IMAGES:**			
NAME:							
ALIAS:							
DOB:							
DL/PID #:							
SID #:				**FBI #:**			
ADDRESS:							
SOCIAL MEDIA:							
INCARCERATION STATUS:	Choose an item.	**SOURCE:**	Choose an item	**DATE:**			
INVESTIGATIVE LEAD PROCESS:	☒ Statewide Network of Agency Photos (SNAP) ☒ DataWorks Plus ☐ Forwarded to Michigan State Police (MSP) for additional assistance						
DATE/TIME FINALIZED:							
CIU PERSONNEL:							
CIU PEER REVIEWER:							
SUPERVISOR:							

REAL TIME CRIME CENTER — FACIAL RECOGNITION INVESTIGATIVE LEAD

The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and **IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT.** Any possible connection or involvement of any subject to the investigation must be determined through further independent investigation and investigative resources. Facial recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the input image's quality, lighting, face angle, and face obstructions, among other factors. Facial recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).

FURTHER INVESTIGATION WAS COMPLETED TO DETERMINE THE NECESSARY PROBABLE CAUSE TO PROCEED WITH AN ARREST OF THE INDIVIDUAL AND/OR SUBMISSION OF A WARRANT:

- ☐ CODIS Match
- ☐ AFIS hit
- ☐ CDR warrant results
- ☐ PEN warrant results
- ☐ Social Media warrant results
- ☐ Witness Statements
- ☐ Other: _____
- ☐ Other: _____
- ☐ Other: _____

INVESTIGATIVE OPERATIONS:

Prior to an arrest of an individual and/or submission of a warrant, the information was reviewed and:

- ☐ APPROVED
- ☐ DENIED

Investigate Operations Captain (print): _____

Signature: _____ **Date:** _____

COMMANDING OFFICER:

Prior to an arrest of an individual and/or submission of a warrant, the information was reviewed and:

- ☐ APPROVED
- ☐ DENIED

Commanding Officer (print): _____

Signature: _____ **Date:** _____

Revised: 12/6/2023

REAL TIME CRIME CENTER — FACIAL RECOGNITION VETTING

The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and **IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT.** Any possible connection or involvement of any subject to the investigation must be determined through further independent investigation and investigative resources. Facial recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the input image's quality, lighting, face angle, and face obstructions, among other factors. Facial recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).

REQUEST DATE/TIME:					
REPORT NUMBER:					
CRIME:	☐Homicide ☐Robbery/Carjacking ☐Aggravated Assault/NFS ☒CSC 1/CSC 3 ☐Home Invasion 1				
REQUESTER NAME:		**RANK:**	Choose an item.	**COMMAND:**	
IMAGE SOURCE:			**NUMBER OF IMAGES:**		
REASON:	☒ Reasonable Suspicion of a Part I Violent Crime or First-Degree Home Invasion ☐ Physical Incapacity/Mental Incapacity/At-Risk Person/Deceased Person (Homicide Only)				
PER POLICE REPORT, SUPPLEMENTS, AND DETECTIVE NOTES:					
PROBE ROLE IN CRIME:	Choose an item.				
SUSPECT KNOWN:	Choose an item.				
PHOTO QUALITY:					
FILE SIZE:			**DIMENSIONS:**		
RACE:			**SEX:**		
FACIAL OBSTRUCTIONS:					
FACE ORIENTATION:					
IMAGE BRIGHTNESS:					
TATTOOS/FACIAL PIERCINGS/BIRTH MARKS:					
NUMBER OF USABLE IMAGES:					
STATUS OF REQUEST:	Choose an item.				
IF REJECTED, WHY?					
ANALYST:			**DATE/TIME:**		
REVIEWER:			**DATE/TIME:**		
SUPERVISOR:			**DATE/TIME:**		

Intel Number:	**23-**

Revised: 12/6/2023

Attachment C

Revised Manual Directive 203.11
Regarding Eyewitness Identification and Lineups

ral

DETROIT POLICE DEPARTMENT MANUAL

FSeries 200 Operations	Effective Date	Review Date *Two Years*	Directive Number **203.11**
Chapter 203 – Criminal Investigations			
Reviewing Office *Investigative Operations*			☐ New ☐ Directive ☒ Revised Revisions in *italics*
References			

EYEWITNESS IDENTIFICATION AND LINEUPS

203.11 - 1 PURPOSE

The purpose of this directive is to establish the guidelines for eyewitness identification *procedures involving showups, photo arrays, and live lineups. Erroneous eyewitness identifications have been cited as the factor most frequently associated with wrongful convictions. Therefore, in addition to eyewitness identification, all appropriate investigative steps and methods should be employed to uncover evidence that either supports or eliminates the suspect identification.*

203.11 - 2 POLICY

Members shall strictly adhere to this directive in order to maximize the reliability of identifications, minimize *erroneous identifications, and gather evidence that conforms to established legal procedures.*

203.11 - 3 Definitions

203.11 - 3.1 *Administrator*

The law enforcement official conducting the identification procedure.

203.11 - 3.2 *Double-Blind Presentation*

The administrator conducting the identification procedure does not know the suspect's identity.

203.11 - 3.3 *Filler*

A live person, or a photograph of a person, included in an identification procedure who is not considered a suspect.

203.11 - 3.4 *Live Lineup*

The process of presenting live individuals to an eyewitness for the purpose of identifying or eliminating suspects.

203.11 - 3.5 *Photo Array*
A means of presenting photographs to an eyewitness for the purpose of identifying or eliminating suspects.

203.11 - 3.6 *Sequential*
Presentation of a series of photographs or individuals to a witness and or a victim one at a time.

203.11 - 3.7 *Showup*
The presentation of a suspect to an eyewitness within a short time frame following the commission of a crime to eliminate them as a possible perpetrator. Showups, sometimes referred to as field identifications, are conducted in a contemporaneous time frame and proximity to the crime.

203.11 - 3.8 *Simultaneous*
Presentation of a series of photographs or individuals to a witness and or a victim all at once.

203.11 – 3.9 *Victim*
For purposes of this directive, an individual who is allegedly the victim of a crime and who also meets the definition of Witness under this policy.

203.11 – 3.10 *Witness*
For purposes of this directive, an eyewitness, meaning an individual who saw the suspect in person.

203.11 - 4 Procedures

203.11 - 4.1 *Showups*
The use of showups should be avoided whenever possible in preference to the use of a live lineup or photo array procedure. However, when circumstances require the prompt presentation of a suspect to a witness and or a victim, the following guidelines shall be followed to minimize potential suggestiveness and increase reliability:

a. *Document the witness's and or a victim's description of the perpetrator prior to conducting the showup. This description should be clearly noted as the witness and or victims' description and separate from the description noted by the member;*
b. *Conduct a showup only when the suspect is detained within a reasonable time frame after the commission of the offense and within a close physical proximity to the location of the crime;*
c. *Members shall obtain supervisory approval before conducting a showup;*

203.11 Eyewitness Identification and Lineups

d. *Do not use a showup procedure if probable cause to arrest the suspect has already been established;*
e. *Transport the witness and or the victim to the location of the suspect whenever possible. Members shall not transport the suspect to the witness and or victim;*
f. *If possible, avoid conducting a showup when the suspect is in a patrol vehicle, handcuffed, or physically restrained by Department members, unless safety concerns make this impractical;*
g. *Do not take a suspect to the witness's and or victim's residence unless it is the scene of the crime and without the consent of both the suspect and the witness or victim;*
h. *Caution the witness and or victim that the person they are about to see may or may not be the perpetrator – and it is equally important to clear an innocent person. The witness and or victim should also be advised that the investigation will continue regardless of the outcome of the showup;*
i. *Do not conduct the showup with more than one witness and or victim present at a time;*
j. *Separate witnesses and or victims and do not allow communication between them before or after conducting a showup;*
k. *If one witness and or victim identifies the suspect, use a live lineup or photo array for remaining witnesses;*
l. *Do not present the same suspect to the same witness and or victim more than once;*
m. *Do not require showup suspects to put on clothing worn by, speak words uttered by, or perform other actions of the perpetrator;*
n. *Members should avoid words or conduct of any type that may suggest to the witness and or victim that the individual is or may be the perpetrator;*
o. *Remind the witness and or victim not to talk about the showup to other witnesses and or victims until police or prosecutors deem it permissible;*
p. *Videotape the identification process using an in-car or body-worn camera;*
q. *Members shall not use a cellular phone or other mobile communication device for a showup; and*
r. *Members shall document the time and location of the showup, the members present, the result of the procedure, and any other relevant information on their officer's daily report.*

203.11 - 4.2 *Basic Procedures for Conducting a Live Lineup or Photo Array*

1. *A live lineup or photo array may only be administered to a witness and or victim as defined in this policy.*
2. *Prior to conducting a live lineup or photo array, members shall have the witness and or victim provide a recap of the incident to provide clarity that the witness and or victim has actual recollection of the incident and the suspect.*
3. *Prior to conducting a photographic line-up, a supervisor shall ensure that there is an independent basis supported by reliable evidence that the suspect, who will be presented in the line-up, committed the crime. An investigative lead generated by a search using facial recognition technology does not alone constitute an independent basis that the person selected as the lead committed the crime.*
4. *The photographic lineup shall not contain an image derived from facial recognition.*
5. *All photo lineups will be conducted using the sequential, double-blind presentation technique to ensure effective eye-witness identification. This means that an investigator, other than the lead investigator, who does not know who the suspect is, will present the line-up to the witness and or victim. It also means that photographs will be presented one-by-one to the witness and or victim.*
6. *The live lineup or photo array should consist of a minimum of six (6) individuals or photographs. Use a minimum of five (5) fillers and only one suspect.*
7. *Fillers should be reasonably similar in age, height, weight, and general appearance and be of the same sex and race, in accordance with the witness's and or victim's description of the offender.*
8. *Avoid the use of fillers who so closely resemble the suspect that a person familiar with the suspect might find it difficult to distinguish the suspect from the fillers (i.e., twins, look-alikes, facial recognition derived images, etc.).*
9. *Create a consistent appearance between the suspect and the fillers with respect to any unique or unusual features (e.g. scars, tattoos, facial hair) used to describe the perpetrator by artificially adding or concealing that feature on the fillers.*
10. *If there is more than one suspect, include only one in each live lineup or photo array.*
11. *During a double-blind presentation, no one who is aware of the suspect's identity should be present during the administration of the photo array. However, during a live lineup, the witnessing attorney should be present.*
12. *Place suspects in different positions in each live lineup or photo array.*
13. *Neither witnesses nor victims should be permitted to see or be shown any photos or images of the suspect prior to or during the live lineup or photo array other than the photo of the suspect included in the photo array at the time it is administered.*
14. *The live lineup or photo array should be shown to only one witness and or victim at a time; in order to prevent participating witnesses and or victims from being aware of the responses of other witnesses and or victims, members should separate witnesses and or victims and warn them not to communicate with each other about the lineup or images involved in the lineup until all witnesses and or victims have completed the live lineup or photo array.*

15. *Multiple identification procedures should not be conducted in which the same witness and or victim views the same suspect more than once.*
16. *Members shall not use statements, cues, casual comments, or provide unnecessary or irrelevant information that in any manner may influence the witnesses' and or victim's decision-making process or perception. In investigations where facial recognition technology was used prior to the lineup, members shall not inform the witness or victim that facial recognition technology was used or that it generated information contributing to the inclusion of an individual in the lineup.*
17. *The proceeding must be conducted in a fair manner, so as not to be unduly suggestive of the suspect. This is important because any remarks could later be interpreted as an attempt to influence the identification.*
18. *The administrator shall ask the witness and or victim to complete and sign a live lineup or photo array form at the time of the lineup. As part of the form, the witness and or victim shall record their degree of confidence in their identification.*
19. *Live lineup and photo array procedures shall be video and audio recorded, unless doing so is not possible. If a procedure is not recorded, a written record shall be created and the reason for not recording shall be documented. In the case of live lineups that cannot be recorded, members shall take and preserve a still photograph of each individual in the lineup.*
20. *The administrator shall document all parties present during the live lineup.*

203.11 - 4.3 *Photographic Arrays*

Prior to conducting a photographic lineup, a supervisor shall ensure that there is an independent basis supported by reliable evidence that the suspect, whose picture is to be presented in the course of the photo lineup, committed the crime. An investigative lead generated by a search using facial recognition technology does not alone constitute an independent basis.

1. *When creating a photo array, members shall follow the below guidelines:*
   a. *Do not use a facial recognition derived image;*
   b. *Use photos contemporary to when the crime occurred;*
   c. *Use black and white photos only if there are no color photos available;*
   d. *Do not mix color and black and white photos;*
   e. *Use photos of the same size and basic composition;*
   f. *Never mix mug shots with other photos;*
   g. *Do not include more than one photo of the same suspect; and*
   h. *Cover any portions of mug shots or other photos that provide identifying information on the subject – and similarly cover other photos used in the array.*
   i. *Do not use images of people who so closely resemble the suspect that a person familiar with the suspect might find it difficult to distinguish the suspect from the fillers (i.e., twins, look-alikes, facial recognition derived images, etc.).*

2. *The sequential procedure process should be preserved as part of the case file.*
3. A *witnessing* attorney *must* be present if a witness and or victim views photographs when the suspect is in custody. *Members shall obtain the attorney's information including their name, phone number, address, and state bar number.*
4. The attorney shall initial photocopies of all photographs used in the *photo array.* The officer in charge of the case shall ensure that attorneys witnessing the photo *array* are provided with a document outlining the attorney's role at the photo show up.
5. Where a witness and or victim identifies the suspect through the use of photographs, the "totality of the circumstances" test is used to determine whether the photographs utilized are not unnecessarily suggestive of any particular suspect.

203.11 - 4.4 *Live Lineups*

1. *When conducting the live lineup, members shall follow the below guidelines:*

   a. *The administrator of a live lineup must be a blind administrator who does not know the identity of the suspect;*
   b. *Ensure that all persons in the live lineup are numbered consecutively and are referred to only by number; and*
   c. *Document all parties present at the live lineup.*

2. *The officer in charge of the case is responsible for the following:*

   a. *Scheduling the live lineup on a date and at a time that is convenient for all concerned parties, to include the witnessing attorney and any witnesses and or victims;*
   b. *Ensuring compliance with any legal requirements for transfer of the subject to the live lineup location if they are incarcerated at a detention center; and*
   c. *Making arrangements to have persons act as fillers.*

3. A written record, the *Lineup* and Photo Identification Record (DPD355), should include:
   a. Names, *age,* and addresses of all persons whose photographs are to be used in the *live lineup or photo array;*
   b. Physical description of all persons whose photographs are to be used in the *live lineup or photo array;*
   c. Names and addresses of all persons present at the *live lineup or photo array;*
   d. Statements of identifying witnesses and or victims while making the identification; and
   e. *The witness's and or victim's degree of confidence in their identification, as specified above in 203.11 – 4.2(18).*

4. A *live* lineup cannot be avoided by having a witness and or victim view photographs when a formal *live* lineup is *reasonably* possible. *A photo array shall* not *be* conducted if the suspect is in custody, unless:
   a. It is not possible to arrange a proper lineup;
   b. There are an insufficient number of persons available with the defendant's physical characteristics;
   c. The nature of the case requires immediate identification;
   d. The witnesses and or victims are *physically unable to attend a lineup*; or
   e. The subject refuses to participate in a lineup and by this action would seek to destroy the value of the identification.

5. All live lineups shall be photographed.
   a. The name, rank, and assignment of the *member* taking the photograph shall be entered on the *Lineup* and Photo Identification Record (DPD355), in the box designated "OTHERS PRESENT." The photograph shall then be attached to the *Lineup* and Photo Identification Record and become a permanent part of the court file.
   b. The officer in charge of the case shall be responsible for the photographing of lineups conducted at all other locations.

203.11 - 4.5 Refusal of Detainee to Stand in a Lineup

1. If a detainee refuses to stand in a lineup, the following procedures shall be followed:
   a. A determination shall be made as to the availability of a photograph of the detainee suitable for use in photograph identification; and
   b. Photograph identification can be used in lieu of a lineup if the subject refuses to participate in a lineup and, by the subject's action, would seek to destroy the value of the identification.

2. Regardless *of* whether a photograph is available or not, between the hours of 8:30 a.m. to 4:30 p.m. on weekdays and from 8:30 a.m. to 1:00 p.m., on Saturdays, Sundays, and holidays, the Wayne County Prosecutor's Office shall be contacted. *At any other time*, the Control Desk shall be contacted for the number of the on-duty assistant prosecuting attorney.
3. The prosecuting attorney contacted shall be informed if a photograph of the detainee is available or not and shall be informed that the detainee refuses to participate in a lineup. Department members and detention personnel shall be guided by the advice of the prosecuting attorney. Although the Michigan Supreme Court has ruled that forced participation in a lineup does not constitute unreasonable search and seizure, no force shall be exerted to force participation of a detainee in a lineup unless the prosecuting attorney contacted gives direction for such action.

203.11 - 4.6 *Limited Use of Video for Identification Purposes*

Members shall only utilize video to confirm the identity of a subject should the witness and or victim be a close associate or family member of the subject (e.g. mother / father or close friend).

203.11 - 5 Witnessing Attorney

1. *A witnessing attorney shall be present for all live lineups and photo arrays when the suspect is in custody.*
2. *Should the suspect be criminally charged and have obtained a lawyer, then the suspect's defense attorney shall act as a witnessing attorney. In all other cases, the officer in charge of the case shall call Notification and Control who shall identify the witnessing attorney.*
3. The purpose *of the witnessing attorney*'s presence is not to interfere with the conduct of the *live* lineup or *photo array* but to observe the procedures used by the law enforcement officers, so that in any subsequent court proceeding the accused will have a lawyer as a witness to any unfair suggestive procedures that may have been employed during the lineup or *photo array*.
4. Under no circumstances may a lawyer interfere with the conduct of the *live* lineup. While counsel may advise a client not to make incriminating statements, counsel may not advise a client to refuse to participate in the *live* lineup or any requested physical demonstrations *including a voice test, a handwriting sample, to wear certain clothing to assume a stance, to walk or to gesture*. If any lawyer should so advise a client, the Prosecuting Attorney's Office should be notified so that appropriate action may be considered.
5. *The OIC's responsibility is to document any objections, procedural violations, or other concerns voiced by the witnessing attorney during the live lineup or photo array.*

Attachment D

Training Provisions

Training Provisions for Settlement in *Williams v. City of Detroit*

1. The Detroit Police Department (DPD) will continue its current practice of requiring all newly promoted or newly hired detectives to complete a detective training school (currently known as the Detective Promotional Assessment Course (DPAC)). In addition to its current components, the detective training school shall include:
    a. A unit on the basics of how facial recognition technology functions, what features of a probe image can affect the reliability of the result of a facial recognition search, and why facial recognition technology alone should not be relied on for a positive identification;
    b. A unit on all of the requirements of DPD's manual directive on facial recognition;
    c. A unit on all of the requirements of DPD's manual directive on eyewitness identification and lineups.
2. DPD shall provide its sworn officers with training on the manual directives for facial recognition and for eyewitness identification and lineups as part of their annual in-service training. Training on both policies will also be incorporated into the training programs for new sergeants and lieutenants (SPAC and LPAC programs).
3. DPD shall train detectives, investigators, or supervisors of detectives and investigators stationed in each precinct detective unit (PDU) that utilize facial recognition technology on how facial recognition technology functions.
    a. The facial recognition training shall include training on the following subjects:
        i. That a facial recognition investigative lead is not a positive identification;
        ii. The basic steps that occur in a one-to-many facial recognition search, the image databases that are searched by each algorithm and what type of photos are contained in each database, the standards by which the system identifies possible matches, and the human process of morphological comparison that follows;
        iii. The fact that the accuracy of a facial recognition result depends on the probe image's quality, lighting, face angle, and face obstructions, among other factors;
        iv. The requirements of Manual Directive 307. 5-3, 307.5-4, 307.5-5.3, 307.5-5.4;
        v. Understanding the Investigative Lead Report and the Vetting Report.
        vi. The fact that studies have shown that facial recognition technology is not as accurate at identifying people with darker skin tones as it is at identifying white people.
    b. The facial recognition training shall be conducted by one or more trained facial recognition examiner(s) trained in the technical and operational details of the facial recognition system utilized by the Detroit Police Department and Michigan State Police.

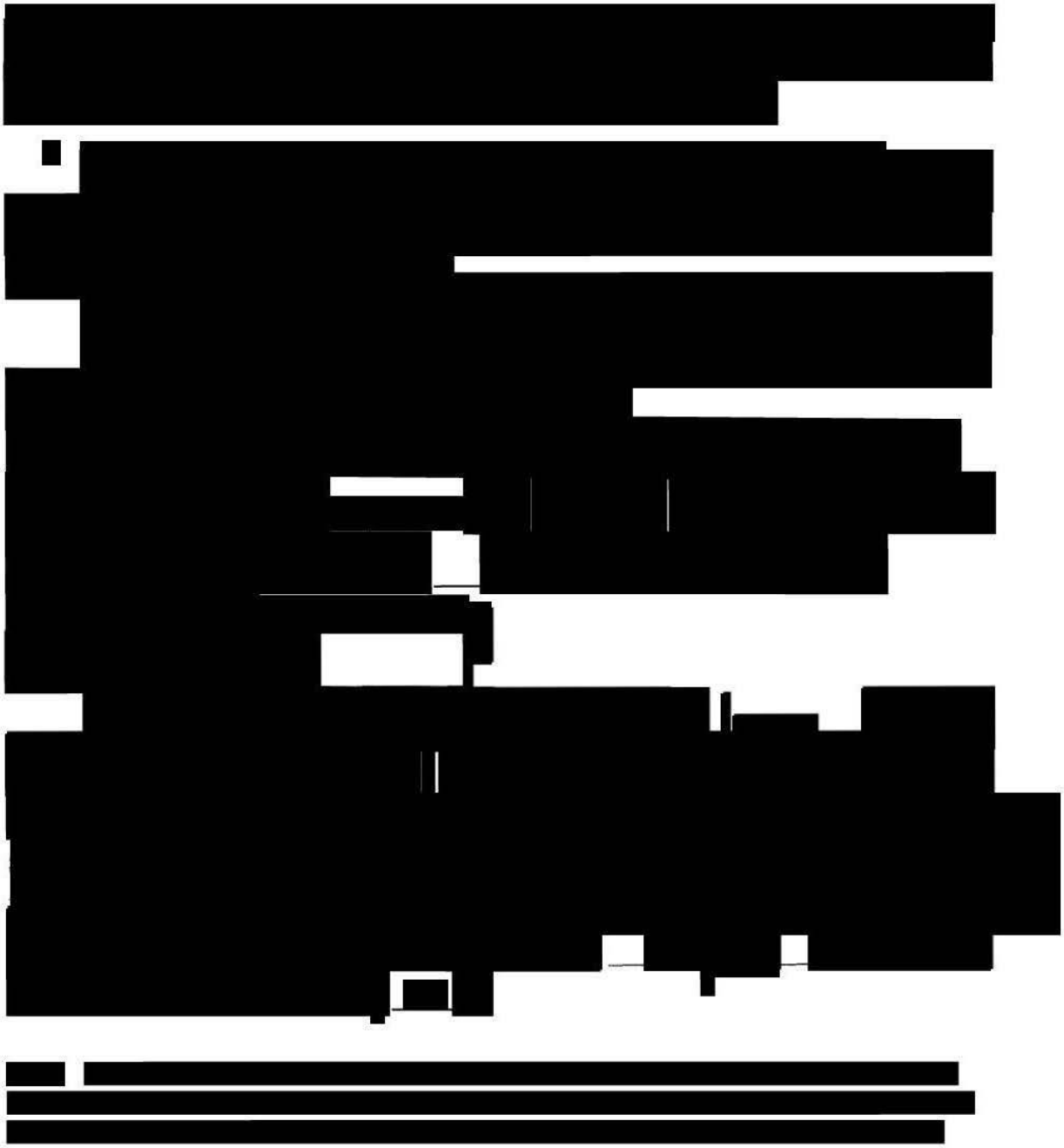
c. DPD shall complete training under this section within one year of the date of this Agreement for all currently active detectives, investigators, or supervisors of detectives and investigators stationed in each precinct detective unit (PDU) that utilize facial recognition technology. This one-year timeline shall not include training of any sworn members who are unavailable for training due to an approved long-term leave of absence, including but not limited to members unavailable due to military service, disability, suspension, or family-emergency-medical-leave. Those members shall be trained as soon as practicable upon their return to active service with DPD.

Attachment E

General Release

GENERAL RELEASE

[redacted]



Statement of Commissioner Adams

I voted in favor of this report for several reasons, but I want to be clear that I do not consider this report the last word on the issue, but merely a beginning regarding examinations of the role Facial Recognition Technology (FRT) should play in society.

Two issues dominate the conversation on the FRT issue: the accuracy of the technology and the danger its potential misuse by the government presents to free speech and civil liberty. This report's focus is on the challenges regarding the accuracy of the technology in pursuing criminals and protecting national security and public safety. It does not go into much depth regarding the danger FRT poses to those who use their freedom of speech or protest to non-violently dissent from government viewpoints. In fact, the greater FRT's technical accuracy the greater the threat from the government's potential misuse of it poses to political freedom and dissent.

This report does not address such civil liberty concerns, so I want to be clear that my vote for this report does not mean I endorse the use of FRT by government to mass surveil the public at large in general or for their political speech or exercise of their other First Amendment rights.

In regard to the focus of this report on the use of FRT by the federal government and DOJ, DHA, and HUD particularly, I want to agree with several issues that were identified. Most importantly, no law enforcement action should be taken against suspected criminals based *solely* on an FRT match – such matches need to be combined with other information and investigation to determine probable cause and an individual's guilt or innocence.

In addition, the federal government should require that federal, state and local governments using federal funds to purchase FRT technology use technology that has demonstrated through testing a high degree of accuracy in its results across demographics. In addition, those officials who actually use the technology should be trained in its use including its shortfalls. Finally, FRT use by government personnel should be subject to oversight by higher ranking officials to protect against misuse.

No technology is perfect, but as the report notes, FRT proponents say it is more accurate than eyewitness testimony – which is a good thing. However, the increasing use of FRT by government means that policy makers need to set guardrails against its misuse – intentional or not.

I do not think there is a consensus on the FRT issue from the left or the right, but the report provided useful insight as to facts and concerns about the issue, and thus moved the public debate forward. That is why I voted for it. That is unlike many past reports from the Commission which have clearly taken the progressive view of issues by providing facts that support those views while discounting facts that do not, at the cost of the ideological balance the Commission was created and charged with pursuing.

[This page is left intentionally blank]

Statement of Commissioner Gilchrist

The Commission's adaptation of the Facial Recognition Technology (FRT) briefing was one of the most enlightening briefings I've had since being on the Commission for the past three years. I thought it was relevant and timely. All our topics touch upon the lives of the American people in some way, but this topic seems to be progressing ahead of our government's ability, capacity or willingness to respond responsibly. Technology is rapidly changing, and this report serves as another reminder about the importance of this issue. Facial recognition technology has tremendous possibilities for good, yet we must be cognizant of the harms that FRT presents. As Artificial Intelligence (AI) continues to become a major factor in our lives, it's imperative that governments maintain some oversight of this rapidly changing technology that's making major decisions our lives. Al technologies are deciding who gets hired or fired, who gets a loan for a car or a house, or as its related to FRT, who gets access or denied access, who gets detained or jailed because of accurate or inaccurate identification.[704] These decisions are increasingly made by algorithms.

Law enforcement's use of FRT to help solve crimes, particularly violent crimes, is a good thing for our society. As a father, I would want every tool available to apprehend someone that has hurt my loved one's. FRT has also been used to capture exploiters of children, fraudsters and violent criminals. Expert testimony from Clear View CEO, Hoan Ton-That was persuasive in his defense of FRT to help law enforcement solve crimes:

> ***Our products are used by law enforcement and government agencies to solve crimes such as child exploitation, murder, money laundering and financial fraud as well as investigating threats to national security. It's used actually in an after the fact forensic matter done in a real-time way and it only serves as public information collected from the internet.***[705]
>
> ***Our technology has been proven to be extremely effective to law enforcement. For example, our technology played an essential role in the investigation that followed the storming of the capital on January 6 by helping law enforcement agencies investigate unidentified persons pictured engaging in violence that day***.[706]

I especially appreciated Mr. Hoan Ton-That's real-world example of how FRT can have a direct impact in assisting law-enforcement in solving some difficult crimes. His testimony continued…

> ***I would like to take this time to share two examples here of the positive use cases in facial recognition technology.***
>
> ***The first example here that you can see on the poster on the right is the child exploitation case. In 2019, Homeland Security investigations were trying to identify an adult male who was molesting a 7-year-old girl and sharing the abuse video online. His face just happened to be in the video***

[704] Ananya. Algorithms Are Making Important Decisions. What Could Possibly Go Wrong? Retrieved September 7, 2023, from https://www.scientificamerican.com/article/algorithms-are-making-important-decisions-what-could-possibly-go-wrong/
[705] Hoan Ton-That. "Testimony Before the U.S. Commission on Civil Right." Transcription, March 8, 2024. pg. 29
[706] IBID

> ***accidentally for just a second. They had no other clues or ways to identify the perpetrator, so they turned to Clearview AI.***[707]
>
> ***The top left photos as you can see is what they called probe condition, which is an image that law enforcement is trying to identify. That photo was uploaded to Clearview AI to search the public internet and what came back as just one single image, which is the one on the right. You can see that the suspect is actually in the background of that photo.***[708]
>
> ***From the second photo, the investigators learned two clues. Firstly, it was posted in Las Vegas. And secondly the name of the employer where the suspect worked. From those two clues, they were able to talk to the employer, find the name and get further evidence to get a search warrant.***[709]
>
> ***So this is the story of Andrew Conlin. Andrew Conlin was facing 15 years in jail for vehicle manslaughter that he did not commit. He was a passenger in a horrific accident where the driver was killed, ejected from a vehicle quite a while ago.***[710]
>
> ***A Good Samaritan came to the scene to rescue Andrew Conlin out of the passenger seat. The police then arrived and questioned the Good Samaritan but forgot to get his contact information. But there was body cam footage of him. Later on, the prosecutor wrongfully accused Andrew of being the driver, and he was charged with vehicle manslaughter and facing 15 years for a crime he did not commit. His public defender was trying to find and identify who this Good Samaritan was from the body cam footage to try and have him testify.***[711]
>
> ***He tried everything, posters, appeals to the public and so on. Eventually they turned to Clearview AI. Clearview AI was able to find a lead of the Good Samaritan at a party in Florida on a web page. With some other investigative work, they got a name and a phone number. And once he heard the story, he was able to testify about what really happened that day, and the charges against Andrew Conlin were dropped.*** [712]

I also found the testimony of Armando Aguilar, Assistant Chief, City of Miami Police Department to be quite illuminating as well. The city of Miami was able to improve its crime rates by effectively implementing artificial intelligence (AI) within their departments. Chief Aguilar explains:

> ***The Miami Police Department has successfully leveraged artificial intelligence over the past years to great effect. We use gunshot detection systems, public safety cameras, facial recognition technology, or FRT, video analytics, license plate readers, social media threat monitoring and mobile data forensics.***[713]

It's quite clear that FRT is a powerful tool! The usage of this tool by our government, particularly our law enforcement apparatus has aided in solving and capturing perpetrators of crimes in less time than before the incorporation of AI tools, including FRT.

---

[707] IBID
[708] IBID pg. 30
[709] IBID
[710] IBID pg. 31
[711] IBID
[712] IBID pg. 32
[713] Armando Aguilar. "Testimony Before the U.S. Commission on Civil Right." Transcription, March 8, 2024. pg. 36

I'm fortunate to have been one of the Commissioners, that had an opportunity to visit the Department of Homeland Security Lab, Maryland Test Facility (MdTF), a 24,000 square foot laboratory space fully instrumented and designed for scenario testing of biometric systems using human subject testing.[714] This onsite visit was very illuminating. At the time of our visit, real human test subjects were present, and I was able to witness firsthand how the testing process was implemented gave me tremendous insight into how scenario testing is done. As mentioned in this report the goals from the MdTF operations includes:

> ***1) driving efficiencies by supporting cross cutting methods and best practices, 2) delivering subject matter expertise across the DHS enterprise, 3) engaging the industry and providing feedback, and 4) encouraging innovation with industry and academia***.[715]

I was encouraged that the government's goals of engaging the private sector and encouraging the private industry with valid feedback on effectiveness, accountability and accuracy is the kind of collaboration that's needed to ensure that FRT technology meets minimum standards.

There are a couple things that I believe are worth mentioning that are alarming. While I do not want to limit the power of the private sector to innovate and help us solve problems more quickly and accurately, we must ensure that's its done with respect for the civil liberties and civil rights of all Americans. The accumulation of mass data collected on the American people is astounding! It's estimated that more than 119 million Americans are in some form of facial recognition database.[716] It's not just that our government is surveilling innocent American citizens; we, the public, know very little about how this data is stored, who has access to it, but not the least important, how is this data being used? In an age where American's data is being compromised continuously, how is it that we can honor innocent people's right to privacy when so many intrusions are occurring? I share Representative Jim Jordan's concerns regarding FRT stated at an Oversight Committee hearing five years ago:

> ***We learned some important things about facial recognition technology there are all kinds of mistakes made when it's implemented those mistakes disproportionately impact African-Americans. There are First Amendment and Fourth Amendment concerns when its used by the FBI and the federal government. There are due process concerns when its used by the FBI and the federal government. We learned that over 20 states have given their Bureau of Motor Vehicles Department their drivers license database. They've just given access to the FBI and no individuals signed off on that and when they renewed their drivers license, they didn't sign off on that. They didn't sign any waiver saying, "oh" its okay to turn my information, my photo over to the FBI. No elected officials voted to allow that to happen, no state assemblies, no General Assemblies, no bills, no Governor signing something, no bill to say its ok for the FBI to have this information…***[717]

---

[714] The Maryland Test Facility, https://mdtf.org/.
[715] U.S. Dep't of Homeland Security, Science & Technology Directorate, Site Visit Presentation at MdTF, Apr. 18, 2024.
[716] Lee, Betram. "Testimony Before the U.S. Commission on Civil Rights." Transcription, March 8, 2024. pg. 22
[717] Jordan, Jim. "Facial Recognition Technology (Part II): Full Committee. Youtube, uploaded by GOP Committee on Oversight and accountability, 04 June 2019, https://youtu.be/ZGfj_JhiNIc?si=I88voXf71om8ZGAX

One of the most troubling issues concerning FRT technology is accuracy. While the accuracy rates of FRT technology have improved dramatically over the past five years, there are still discrepancies. Unfortunately, those discrepancies are more prevalent on brown-skinned persons, women and the elderly. The accuracy issues of FRT technology are more than about the algorithms. It's also about the lighting, camera angle, the picture quality and the interpreter of the images.[718] When the government utilizes FRT technology tools it's imperative that they do so with tremendous care and responsibility. For instance, in Detroit, Michigan the government arrested three people after faulty facial recognition matches.[719] One case that specifically captured the public's attention when 32-year-old Porcha Woodruff was arrested for carjacking and robbery. While getting her two kids ready for school one morning, six Detroit police officers had a warrant for her arrest. According to her lawsuit she was handcuffed, booked and jailed. Woodruff's complaint alleged she was implicated after facial recognition was used after the carjacking victim identified her in a lineup of photos that included a previous mugshot arrest of her. But Chief White of the Detroit Police Department claims it was not the technology that was the issue, but bad investigative police work.[720]

> ***"I have no reason to conclude at this time that there have been any violations of the DPD facial recognition policy, however, I have concluded that there has been a number of policy violations by the lead investigator in this case. What this is, is very, very poor investigative work that led to a number of inappropriate decisions being made along the lines of the investigation, and that's something this team is committed to not only correcting, having accountability, having transparency with this community, and in building policy immediately to ensure regardless of the tool being used, this never happens," White said***.[721]

When you look closer at many of these misidentification issues, inadequate investigative work is more often the culprit than the FRT technology itself. However, FRT is being overly relied upon in cases where this technology isn't wholly designed to replace trained human interaction. This "automation bias"[722] can cause some serious mistakes. I remember when the usage of global positioning satellite (GPS) systems became ubiquitous. It replaced my big Rand-McNally Atlas maps that were used to navigate the highways. The earlier model of the home/phone GPS software would get you from point A to B fairly accurately, but it didn't always get you exactly there. Today's GPS systems are dramatically more accurate than they were five years ago. But there are times when the system still isn't 100% accurate. Close enough might be good enough for verifying a location, but when it comes to the protection of Americans' constitutional rights, we must work extra hard to get it right. Detaining or arresting someone mistakenly can cause them harm; family disruption, loss of

---

[718] Turner Lee Statement at 4-5

[719] NYTimes.com: Facial Recognition Led to Wrongful Arrests. So Detroit Is Making Changes. https://www.nytimes.com/2024/06/29/technology/detroit-facial-recognition-false-arrests.html?smid=em-share

[720]Yip, Isabel. CNN. "Detroit police chief says 'poor investigative work' led to arrest of Black mom who claims facial recognition technology played a role. August 10, 2023. https://www.cnn.com/2023/08/10/us/facial-recognition-technology-detroit-false-arrest/index.html

[721] IBID

[722] What is Automation Bias? Automation bias is an over-reliance on automated aids and decision support systems. https://www.databricks.com/glossary/automation-bias

income, embarrassment and mental stress.[723] Mistakes are made within any profession, but it's the government's responsibility to get it right and make amends, particularly when one's liberty rights are at stake.

The most surprising discovery was the lack of a plan and oversight from the Department of Housing and Urban Development (H.U.D) regarding FRT. I want to echo my fellow Commissioners Jones and Adams when they admonished HUD for not showing up at our briefing. Commissioner Jones stated the following:

> ***As someone who approached this briefing with an open mind and without any predispositions, I regret that I have had to take a dim view of why these two departments have chosen not to cooperate with the Commission's legitimate inquiry and to their use of facial recognition technology. It suggests to me that DOJ and HUD are embarrassed by their failures and are seeking to avoid public accountability.[724]***

And before the panel of experts began their testimonies, Commissioner Adams, my republican colleague, had this to say:

> ***I want to share Commissioner Jones's concern and support his concern about the absence of DOJ at this hearing. And I would also support any effort you would like to engineer or steer toward obtaining any information from them. I would be wholeheartedly in support of that even if it stands to exercise his subpoena power***.[725]

Based on the responses that H.U.D shared with the Commission from the interrogatories sent by staff it's clear that H.UD. guidance regarding FRT has been inadequate.

> ***[HUD] does not utilize and has not developed any Facial Recognition Technology (FRT). While HUD has no regulations explicitly governing the use of FRT by program participants, HUD requires program participants to use all funds in accordance with Federal, state, and local laws as well as HUD guidelines and regulations***.[726]

> ***HUD does not require specific policies on FRT for Public Housing Authorities (PHA) and does not keep a list of PH.As that elect to use FRT. HUD's funds provide program participants the flexibility to purchase solutions and make investments that will provide decent, safe, and sanitary housing for residents***.[727]

---

[723] Samantha K Brooks, Neil Greenberg. "Psychological impact of being wrongfully accused of criminal offences: A systematic literature review." National Library of Science. 2020 Aug 17, retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7838333/#:~:text=Eight%20main%20themes%20were%20identified%3A%20loss%20of%20identity%3B,employment%3B%20traumatic%20experiences%20in%20custody%3B%20and%20adjustment%20difficulties.

[724] Commissioner Jones. "Testimony Before the U.S. Commission on Civil Right." Transcription, March 8, 2024. pg.12

[725] Commissioner Adams. "Testimony Before the U.S. Commission on Civil Rights." Transcription, March 8 2024. Pg. 14-15

[726] U.S. Dep't of Housing and Urban Development, Response to USCCR Interrogatories

[727] U.S. Dep't of Housing and Urban Development, Response to USCCR Interrogatories.

When vulnerable Americans are being surveilled- not for reasons of protection, but constantly monitored particularly for minor infractions-intimidation can ensue, and very unwelcoming feelings of home is often the result. I want *all* residents- public housing residents or not- to feel safe in their homes and in their communities. I do believe FRT usage as a tool to further facilitate safety is a worthwhile goal, however, that goal can be undermined when abuses or overzealous actions undercuts its legitimate purposes to protect and maintain safety.

Conclusion:

I urge our congressional leaders and the president to pass some reasonable legislation that protects the civil liberties and civil rights of the American people. I agree with Deirdre Mulligan, Principal Deputy U.S. Chief Technology Officer of the White House Office of Science and Technology Policy (OSTP), as she wrote in her statement to the Commission:

> ***If we use this technology, we must use it responsibly—it needs to work, and it needs to protect people's rights, protect their freedoms…and adhere to our fundamental obligation to ensure fair and impartial justice for all. Advances in technology have challenged us before. Each leap in capability brings new opportunities and, with them, new risks. Deciding how and when to use and refuse technology—including facial recognition technology—is a key way our nation manifests our values.***[728]

The use of FRT technology is here and it isn't going anywhere. In places that banned it, are now reincorporating it.[729] In fact, the FRT technology market is expected to grow at an annual rate of 9.34% from 2024 to 2030. It's projected that by the end of 2024, FRT valuation will reach 4.94 billion dollars.[730]

We must ensure that this growth does not parallel with an increased erosion of our civil rights and civil liberties. The lack of federal policy and oversight can lead us further down a dystopian path, like China where they are vigorously and intensely monitoring their population as a means of control.[731] Adequate checks and balances must be put in place to protect our constitutional freedoms. One of the main reasons that America is a great country is because of the freedoms we enjoy, the more we begin encroaching on those freedoms, in exchange for more security, then we quickly begin altering not only our values, but our nation.

---

[728] Mulligan Statement, at 1.
[729] Dave, Paresh. "Focus: U.S. cities are backing off banning facial recognition as crime rises." Reuters. May 12, 2022. Retrieved from https://www.reuters.com/world/us/us-cities-are-backing-off-banning-facial-recognition-crime-rises-2022-05-12/#:~:text=OAKLAND%2C%20Calif.%2C%20May%2012,and%20increased%20lobbying%20from%20developers.
[730] Statista Market Insights. "Facial Recognition – Worldwide." Mar 2024. Retrieved from, https://www.statista.com/outlook/tmo/artificial-intelligence/computer-vision/facial-recognition/worldwide#:~:text=The%20market%20size%20in%20the,US%248.44bn%20by%202030
[731] IBID

Acknowledgements:

This report was able to pass the threshold of strong bipartisanship for most Commissioners due to the subject matter importance, and because of the work of the lead Commissioner, Mondaire Jones and his Special Assistant, Irena Vidulovic. The input and feedback from Commissioners, Special assistants and staff made this report a better document.

I want to thank the entire staff for putting on a very informative briefing and getting this report produced. There are those behind the scenes that help make our jobs as Commissioners possible, thank you! Thank you guys, for your hard work and dedication to vigorously examining civil rights issues that impact our country.

[This page is left intentionally blank]

Statement and Rebuttal of Commissioner Heriot

I abstained from voting on this report. I am embarrassed to say that on July 12, 2024, when the vote was taken, I didn't feel sufficiently on top of the issues that were covered by the report (or by the findings and recommendations in particular) to vote with confidence.

I am embarrassed, but not too embarrassed. One problem was the first draft of the findings and recommendations—all ten pages of them—were not presented to the Commissioners until Wednesday, July 3, 2024, nine days before the vote. I couldn't have gotten on top of them in the amount of time I had if I had tried. I'm not sure anyone could have.

Facial recognition technology and its many uses pose complex issues that are going to require a lot of thought by policymakers—a lot more thought than our Commission and its staff have been able to give them so far. Given the need to publish this report by the end of the fiscal year, however, we had to press on. In the future, I hope the Commission will adopt a procedure for findings and recommendations that begins much earlier. I hope nobody takes these hastily drafted findings and recommendations as the last word on facial recognition technology. They are a first impression by a subset of the Commission at best.

At this point, I think I can make only a few somewhat random comments on the report:

First, I would like to commend Commissioner Mondaire Jones for coming up with the topic. Unlike some of our projects, this one doesn't have a clear left/right feel to it. That makes it a good one for the Commission with its current even split between conservatives and progressives. I just wish we'd all had more time to concentrate on it.

Second, I want to point out how very valuable this emerging technology is (and at the same time how worrisome it is). Some commentators tend to emphasize that the technology is imperfect. But that should be given. Just like everything else in the known universe, it is fallible. That is why it shouldn't be used alone to make an arrest or to conduct a criminal prosecution. I think everyone understands that. Still, while facial recognition by machine occasionally identifies the wrong person, it is massively more accurate than the alternative, which is facial recognition by even more fallible human beings.[732] Juries tend to assume that a positive identification by an eyewitness is extremely

[732] If you want to hear some scary statistics, you'll find them in an article entitled *Policy and Procedure Recommendations for the Collection and Preservation of Eyewitness Identification Evidence*. The authors were a subcommittee of experts selected by the Executive Committee of the American Psychology-Law Society (Division 41 of the American Psychological Association) to undertake an update of an earlier set of guidelines for eyewitness identification procedures. They found:

> [W]e can now estimate how often actual eyewitnesses in serious crime cases mistakenly identify a filler from a lineup. These 11 peer-reviewed published studies collected data from a total of 6,734 lineups. These field studies are from highly varied jurisdictions (e.g. California, Arizona, Texas, London, England) …. For current purposes, two statistics of note … speak to the question of whether actual witnesses to serious crimes are too cautious to make mistaken identification at rates like those observed in lab experiments. First nearly one of every four witnesses (23.7%) who was shown a lineup selected an innocent filler. Second, among those who made an identification (35.5% made no identification), over one third (36.8%) identified a known-innocent filler. A summary of 94 laboratory eyewitness identification studies showed that filler identification rates averaged 21.2%

trustworthy. In reality, however, good-faith errors are frighteningly common. In that respect, facial recognition technology is a gift. It means that fewer innocent individuals will be arrested and sometimes even convicted on the basis of a misidentification by an eyewitness. It also means that fewer crimes will be unsolved. More justice will be done. This is something worth celebrating.

To be sure, efforts should be made to eliminate racial disparities in error rates. But it is important not to lose sight of the fact that overall accuracy is more important. Suppose you have a choice between two different facial recognition technologies to use in the criminal context, one with a 10 to 1 racial disparity in the rates of false positives to overall positive identifications and the other with a 3 to 2 racial disparity.[733] At first glance, one might be tempted to choose the latter technology on the ground that the racial disparity is less, but that temptation should be resisted. Before a choice is made, you're going to want to know what the actual rates of false positives to overall positive identifications are (rather than just the racial disparities in those rates). Suppose the error rate for the first technology is 0.01% for one race and 0.1% for the other.[734] That's a high racial disparity in error rates, but it is an extremely low error rate for both races (or put differently an extremely high accuracy rate for both races)—massively better than what one would get for eyewitness testimony. Suppose the other technology has an error rate of 30% for one race and 20% for another race. The first technology is superior with far fewer members of either race having to suffer the consequences of a false positive. All other things being equal, it should be chosen despite its higher racial disparity.

Chair Garza uses her Statement as an opportunity suggest that the disparity problem is caused by what she calls "the tech industry's mostly white workforce and leadership." She argues that they have "led to the development of technologies that fail to address the needs of diverse communities, thereby deepening existing inequities." I think she misunderstands the situation. First, it is not at all clear that the relevant industry is disproportionately white. For more than a decade, Asian Americans have made up more than half of the tech workforce in Silicon Valley, which is the world's center for

---

when the culprit was present and 34.6% when the culprit was absent (Clark, Howell, & Davey, 2008).

Gary L. Wells, Margaret Bull Kovera, Amy Bradfield Douglass, Neil Brewer, Christian A. Meissner, & John T. Wixted, *Policy and Procedure Recommendations for the Collection and Preservation of Eyewitness Identification Evidence*, 44 Law & Human Behavior 3, 5 (2020).

Between 1989 and 2020, the Innocence Project tracked cases in which DNA evidence was used to exonerate individuals who have been convicted. Out of 375 such cases, 69% involved eyewitness misidentification. Innocence Project, DNA Exonerations in the United States (1989-2020), https://innocenceproject.org/dna-exonerations-in-the-united-states/.

[733] I have left aside the problem of false negatives here. Most Americans agree that our criminal justice system must be willing to put up with a large number of "false negatives" (i.e. failures to convict a guilty person) in order to avoid even one "false positive" (i.e. convicting an innocent person), although they don't always agree on exactly how many. Here we aren't discussing convictions, but rather technology that can be used as evidence and/or to get leads for more evidence in a criminal proceeding and also for other purposes that I can't even predict at this point. I therefore can't yet say anything useful about the false negative problem.

Of course, if we're talking about using facial recognition technology to allow tenants into their apartment buildings, false negatives are a significant inconvenience. I doubt very much that we have a good handle on the many uses of facial recognition technology. That's one more reason I felt uncomfortable endorsing any findings or recommendations.

[734] Note that if we were to "flip it" and talk not about error rates, but rather about rates of true positives to overall positive identifications, the racial disparities are not bad at all. The two figures—99.99% and 99.9% are barely different at all.

technology.[735] Similarly the CEOs of Microsoft, Alphabet & Google, Zoom, Adobe, Broadcom are Asian.[736] The CEO of Clearview, Hoan Ton-That, who testified before the Commission at our briefing is Vietnamese-Australian. But second, and more important, facial recognition technology's problem with racial disparities in error rates is a technical one, not one of cultural nuance. There is no reason to believe that women engineers will be better at improving the technology's accuracy rate for women or that African American engineers will be better at improving its accuracy rate for African Americans. To solve the problem, the most knowledgeable and skillful engineers available are needed. If every one of them were from the same small town in Tamil Nadu, I'd be for that. Alternatively, if they were all from East St. Louis, Illinois, I'd be for that too. In reality, those engineers are diverse along dimensions that go far beyond the race/ethnicity/sex matrix that Chair Garza is concerned with.

I should include a caveat to all this: Facial recognition technology also gives us good reason for worry about the future. If the government can identify a face in the crowd with minimal effort, will it be tempted to identify individuals who participate in protests? Will that cause Americans to fear registering their displeasure with the government? Even under current circumstances, many Americans fear speaking up anywhere but behind closed doors. Will facial recognition technology allow government actors to intimidate dissenters? Will healthy dissent dry up?

These are not just theoretical concerns. China already has an extensive network of cameras and employs facial recognition technology, and its uses of that technology are not something a free society should want to emulate. Somehow our government's ability to use this technology may need to be limited. I don't pretend to know how to accomplish this—not yet anyway. The unsettling thing is that it is very difficult to cause anyone (government officials included) to refrain from using something if they can see a significant advantage in it.

Maintaining a free society is to some degree about maintaining a balance of power between the government and its citizens. Changes in technology are capable of upsetting that balance. Indeed, it happens with some regularity. What role will facial recognition technology ultimately play in that balance of power? I don't know. Right now, I just know that its value in crime fighting is something to marvel at—so much so that King Canute, who knew a thing or two about trying to command the tides to turn back, would laugh at any attempt to ban its use entirely. I'm hoping that in a few years, I will have less need to worry about it on the citizen dissent front. But I am a bit of a pessimist.

[735] See, e.g., Dan Nakaso, Asian Workers Now Dominate Silicon Valley Tech Jobs, San Jose Mercury News, November 29, 2012; Nikhil Inamdar & Aparna Alluri, Parag Agrawal: Why Indian-Born CEOs Dominate Silicon Valley, BBC.com, December 3, 2021.
[736] Daniel Liberto, Legendary Asian American CEOs, Investopedia, May 1, 2024.

[This page is left intentionally blank]

Statement of Commissioner Jones

Artificial intelligence (AI) has its place in almost every facet of modern daily life, from predictive texting to transcription technology, language learning, medical diagnoses, robotics, retail, and space exploration. Facial recognition technology (FRT) is a branch of AI that has seen significant adoption because of its compelling use cases, particularly for its ability to scan massive datasets of facial images for identification purposes. This technology is ubiquitous; facial biometric data can unlock our phones, verify our passport photos at the airport, and surveil our movements in public, among other purposes. Technological innovation like AI is exciting; as its capabilities improve, its use proliferates. However, it is important to recognize that, while the debate surrounding AI's risks and benefits is still emergent, the federal government has nevertheless adopted the technology in a significant way.

The federal government, defined in this report to also include its grantees, is using FRT in a wide range of contexts, including policing, criminal prosecution, homeland security, and even public housing. As use of FRT grows, so does anxiety about how it is developed and deployed. Concerns about oversight, transparency, training, privacy, accuracy, discrimination, and access to justice are at the forefront of these anxieties. The civil rights implications for the use of FRT, especially with respect to communities of color and other marginalized groups, require that this Commission investigate the federal government's utilization of this powerful technology.

I introduced this topic as my first project on the Commission in order to meet this pivotal moment in U.S. history. I proposed this report to review the utilization of FRT by the Departments of Justice (DOJ), Homeland Security (DHS), and Housing and Urban Development (HUD) mindful that FRT has come under scrutiny by civil rights advocates, legislative bodies, and the public generally. This report is the first of its kind in the literature on FRT. It is thus an important contribution to the national discussion on AI generally and FRT specifically. It is also the first time in recent years that the Commission has adopted findings and recommendations as a body that is evenly divided politically. I therefore thank all of my Republican colleagues, especially Commissioner Stephen Gilchrist, for their diligent work in making this project a bipartisan success.

Our investigation was made possible through the independent research conducted by the Commission's brilliant social scientists, our public briefing on March 8, 2024, expert testimony, comments from the public, our site visit to DHS' Maryland Test Facility, and responses to document requests by DOJ, DHS, and HUD. This comprehensive report, including its robust findings and recommendations, is the result of a rigorous, thoughtful effort to uncover the facts and advise the nation.

How Federal Use of FRT Impacts Civil Rights

Through its use of FRT, the federal government is unleashing an extremely powerful technology. In its current adoption across DOJ, DHS, and HUD, including several of their grantees, federal

FRT utilization lacks proper oversight, transparency, training, and testing. As an emerging technology with known bias and accuracy issues,[737] FRT deployed in this imprecise manner takes a human toll. The measured accuracy of FRT systems is not just a datapoint; it represents human lives that are impacted by inaccurate FRT results. As FRT impacts the rights and privileges of Americans, it is a civil rights issue implicating the federal Constitution and various civil rights statutes.

Throughout our investigation, we learned of several instances of FRT inaccuracy and bias impacting the average American, and found that it impacts people of color, women, and older adults disproportionately.[738] Several themes emerged with respect to how federal FRT use may interfere with the rights of Americans; false arrests as a result of police overreliance on inaccurate FRT matches is one such growing concern.[739] The Detroit Police Department falsely arrested Robert Williams, a Black citizen of Farmington Hills, Michigan, in front of his family after two blurry surveillance photos became the basis for a mismatched FRT result, erroneously tying him to a Shinola store robbery in Detroit, an event for which he was not present and was plainly not the perpetrator. The detective with the Detroit Police Department, through omissions in the arrest warrant application, did not put the magistrate on notice that the FRT result underlying the warrant, and the subsequent photo lineup procedure, were not reliable. As a result, the department agreed to an unprecedented settlement that included a significant rollback of its reliance on FRT, and training on the risks of FRT, especially when used on people of color.[740]

Mr. Williams' case illustrates concerns from several experts who testified before the Commission: that, despite using FRT in hundreds of thousands of criminal cases, law enforcement rarely discloses the use of FRT in discovery materials that are used for the defense.[741] Despite its increasing use, there remains no publicly available data regarding the accuracy of law enforcement use of FRT in its actual practice.[742] The lack of visibility into law enforcement's use of FRT, in our criminal legal system where people's lives are at stakes, is a concerning indicator that proper oversight, training, and accountability procedures are not in place.

The use of FRT by DHS across Customs and Border Protection (CBP) and the Transportation Security Administration (TSA) raises civil rights concerns as well. CBP has implemented facial biometrics into the entry processes at all international airports and into the exit processes at 53 airports.[743] The agency has expanded facial biometrics at 40 seaports and all pedestrian lanes at the Southwest and Northern Border ports of entry into the country.[744] Through its Traveler Verification Service (TVS), CBP conducts identity verification using photographs that have previously been

[737] Pgs. 26-31
[738] Pg. 77
[739] Pg. 24
[740] Pg. 88, ACLU https://www.aclu.org/cases/williams-v-city-of-detroit-face-recognition-false-arrest
[741] Pg. 34
[742] Pg. 36
[743] Pg. 57
[744] Pg. 57

provided to the government, such as passport and driver's license pictures. CBP has confirmed that TVS participation is limited to passengers with TSA PreCheck and CBP Global Entry, and that passengers may opt out of the process at any time.[745] Where TSA has deployed its FRT in regular airport screening processes, TSA has stated that passengers may opt out at any time for an alternative, manual security screening, as indicated by signage throughout the airports.[746]

However, questions remain about whether passengers are aware that they have the right to opt out and feel empowered to use it, especially given the imbalance of power between an airport's security administration and an individual passenger. That the signage indicating the right to opt out is typically not prominently displayed or available in several languages further complicates this issue.[747]

Public housing authorities' (PHAs) use of FRT for surveillance is another concerning development. HUD, through its Emergency Safety and Security Grant (ESSG) funding, has facilitated the purchase of FRT and surveillance cameras by PHAs, which are increasingly purchasing this technology to surveil tenants and provide building access in lieu of keys or fobs. PHAs are sharing surveillance footage with local law enforcement agencies, citing public safety as a motivation for this use and claiming that this deters crime and helps identify perpetrators.[748] However, public housing residents, who are disproportionately tenants of color and female, often do not have meaningful alternatives to housing, raising concerns over their meaningful consent to such surveillance. This surveillance can interfere with personal relationships and key social support as tenants and guests are incentivized not to visit or exercise their First Amendment rights to avoid their biometric data being captured by FRT.[749] Considering the inaccuracies of FRT relating to race, gender, and age, its deployment in subsidized housing becomes extremely concerning for civil rights.

Fundamental questions, such as how often the departments and their grantees run searches and for which types of crimes, on which demographics, and to what results, also remain unanswered in the realm of federal FRT use. What little public information does exist about federal law enforcement use of FRT stems largely—sometimes exclusively—from investigative reporting or is scattered across federal auditor reports such as those conducted by the Government Accountability Office (GAO).[750]Additionally, the extent of issues emerging from federal FRT use is unclear, due to a lack of comprehensive data on its use. In HUD's case, the department does not track its grantees' purchase of FRT despite its estimation that 1.2 million households are living in public housing units, managed by 2,756 PHAs.[751] In fact, it was not until April 2023 that HUD announced its ESSG grant funding cannot be used to purchase FRT, a restriction that

[745] Pg. 58
[746] Pg. 39
[747]Pg. 62-63
[748]Pg. 75
[749]Pg. 78
[750]Pg. 37
[751]Pg. 76

does not apply to existing FRT purchases.[752] Information about departmental use of FRT should come from the departments' affirmative commitments to transparency, including publicly available policies, and democratically enacted legislation.

The Federal Response and Legislative Landscape

Over the course of 2022 and 2023, President Biden underscored for the nation the importance of responsible AI use by releasing the Blueprint for an AI Bill of Rights and signing two executive orders (EOs) advancing AI and FRT transparency and accountability. In its Blueprint for an AI Bill of Rights, released in 2022, the White House acknowledged AI's "extraordinary benefits" while emphasizing that this "important progress must not come at the price of civil rights or democratic values."[17753] EOs 14074 and 14110, signed in 2022 and 2023, respectively, included provisions requiring departments to promote accountability, transparency, and trust between law enforcement officials and the public with respect to technology such as FRT and predictive algorithms.[754] They also highlighted the importance of training and technical assistance to those "investigating and prosecuting civil rights violations and discrimination related to automated systems, including AI."[755] Along with the issuance of these EOs, the White House Office of Management and Budget (OMB) established a "rights-impacting" category of AI. Rights-impacting AI, as defined by OMB, includes "AI whose output serves as a basis for decision or action that has a legal, material, or similarly significant effect" on several rights and privileges.[756]

The legislative landscape regarding FRT and AI broadly confirms that official use of this technology is a bipartisan concern, with states passing statutes to limit the use of FRT and members of Congress proposing legislation to do the same. Members of Congress have proposed several bills to address concerns over FRT development and deployment, spanning use cases across law enforcement, customs, and housing.[757] The *Facial Recognition Act of 2023* would place strong limits on law enforcement use of FRT and provide for transparency by requiring annual reporting on the deployment of FRT to protect individuals' rights.[758] The *Traveler Privacy Protection Act of 2023* would prevent TSA from using airports as a site to collect Americans' facial biometric data by repealing current authorization for TSA to use FRT and requiring explicit congressional authorization in the future.[759] The *No Biometric Barriers to Housing Act* would prohibit the use of FRT in most federally funded public housing, requiring HUD to report to Congress how the

[752]Pg. 13
[753]Pg.83
[754]E.O. 14074, *Advancing Effective, Accountable Policing and Criminal Justice Practices To Enhance Public Trust and Public Safety*
[755]E.O. 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*
[756]Proposed Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence. https://ai.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-Public-Comment.pdf
[757]They include: the *Facial Recognition Ban on Body Cameras Act,* the *No Biometric Barriers to Housing Act of 2023*, the *Facial Recognition Act of 2023*, and the *Fourth Amendment is Not For Sale Act*
[758]Pg. 92
[759]Pg. 92

technology impacts the public housing sector and its tenants.[760] These bills, whose sponsors include Democrats, Republicans, and independents, represent just a few of the legislative efforts tackling concerns about FRT and other biometric AI use across the United States.

The Commission's FRT Investigation & Testing Site Visit

While preparing for this report, the Commission held a March 8, 2024 briefing during which we heard from subject matter experts including government officials, academics, researchers, software developers, and legal experts. From March 8 to April 8, the Commission accepted public comments as well. This briefing was a monumental effort to represent the full range of diverse voices on this topic.

At the Commission's briefing, we learned that testing of FRT before deployment was insufficient in terms of accuracy, equitability, and effectiveness. While National Institute of Standards and Technology (NIST) testing examines algorithmic accuracy, it is an entirely voluntary process that does not account for FRT deployed in real-world scenarios, as a component of an entire system.[761] Armed with this expert testimony, we conducted a first-of-its-kind site visit to DHS' Maryland Test Facility (MdTF), a 24,000-square-foot space fully instrumented for scenario testing of biometric systems using human subjects. MdTF operates a "Build Once, Use Widely" testing framework created not only to test, but also to engage the industry and educate AI stakeholders on the current state and challenges of biometric technologies.[762]

During our visit, the Commission focused on how FRT is tested for federal government use for several different testing scenarios. This "scenario testing" provides insight into how an FRT system may work if deployed in the field, allowing vendors to test their systems prior to being used in the real world, where costly mistakes can also lead to civil rights concerns should there be high false match rates for protected classes.

DHS is the only department known to be testing FRT in this way. Despite being open since 2014, the MdTF has not had meaningful engagement from members of Congress and has had limited engagement from other departments within the executive branch.[763] The MdTF represents a promising model for proactive, holistic FRT testing that accounts for the challenges that occur when FRT, which may perform extremely well in laboratory settings, is applied to complex, real-world scenarios where civil rights are at stake. Testing frameworks like the MdTF's, coupled with informed guardrails for FRT deployment, would empower federal departments to proactively test FRT. Making such testing mandatory would allow the federal government to prioritize meaningful oversight that supports innovation while protecting the civil rights they are legally bound to protect.

[760]Pg. 91
[761]Pg. 26
[762]Pg.10
[763]Pg. 10

What We Learned

There are currently no federal statutes or regulations expressly authorizing or limiting FRT use by the federal government. While interim policies for FRT use exist, as of August 2024, there is no official, standardized policy published for federal FRT use.

Lack of transparency and oversight are significant issues for federal FRT use. Of the departments we studied, only DHS has published a department-wide FRT directive.[764] As of July 2024, DOJ has recently adopted an interim FRT policy,[765] while HUD does not track FRT use at all.[766] One of the most significant issues with FRT today concerns its accuracy and bias, but due in part to the lack of oversight and transparency, there are no comprehensive data available regarding the real-world accuracy of FRT as it is used by the federal government. Even with the highest-performing algorithms, tests have shown there are likely to be false positives for certain demographic groups, specifically Black people, people of East Asian descent, women, and older adults.[767] This risk of algorithmic error could be reduced if departments only used algorithms that exhibited high overall accuracy rates and eliminated tested-for accuracy biases.[768] We found that one of the important factors in reducing these biases appears to be the selection of data used to train algorithmic models.

One of our most significant findings is that FRT training as it exists today is insufficient for both the technology and those responsible for operating it. For the technology itself, if algorithms are trained on data sets that contain very few examples of a particular demographic group, the resulting model will be worse at accurately recognizing members of that group in real-world deployments.[769] Testing whether algorithm training is effective and equitable is critical, and promising testing frameworks for this technology do exist. DHS, through its Science and Technology Directorate, funds FRT research, testing, and evaluation at the MdTF, explored extensively throughout our report. MdTF's specialized scenario testing, structured in a "Build Once, Use Widely" format, simulates the full biometric system, testing how FRT performs in its intended use.[770] We found that DHS is the only department known to be testing FRT in this way.[771]

For FRT operators, analysts, and decisionmakers, "trickle-down," compliance-based training modeled after typical annual agency trainings are not sufficient to provide the education and guidance required work with FRT.[772] Federal regulators, enforcement agencies, and the departments deploying the FRT need comprehensive training on the technology and its bias in order to develop a culture of responsible use.[773] Our recommendations focused heavily on

[764]Pg. 64
[765]Pg. 51
[766]Pg. 13
[767]Pg. 27
[768]Pg. 31
[769]Pg. 32
[770]Pg. 67
[771]Pg. 10
[772]Pg. 96
[773]Pg. 95

establishing and incentivizing the adoption of transparent national training standards.

According to the experts who testified before the Commission, the absence of standards for FRT use pervades the entire pipeline, from the designers and developers of the core technology to law enforcement agency policies, to training for the officers and prosecutors who rely on the technology.[774] The overarching concern is that the U.S. lacks the regulatory and financial incentive structure, as well as the necessary levels of transparency and internal expertise to make the necessary changes to establish proper standards, training, oversight, and transparency.[775]

Recommendations

The Commission's recommendations encompass not only legislative action, but also departmental action in the areas of procurement, testing, training, transparency, and oversight.

Congressional Action. The Commission recommends that proper testing and training should be top of mind for any serious legislative action governing the use of FRT. Congress should direct and empower the NIST to 1) develop an operational testing protocol that departments can use to assess how effective, equitable, and accurate their FRT systems are when actually deployed, and 2) condition the receipt of federal funds by grantees on the adoption of national training standards for individuals who review and analyze the results returned by FRT algorithms before those results are shared with investigators. To complement these guardrails, Congress should provide a statutory mechanism for legal redress by individuals harmed by misuse or abuse of FRT. Legislation should include meaningful enforcement for statutory violations, such as civil damages for any person injured as a result of a violation.

Chief AI Officer Actions. The recommendations coming out of recent executive orders, such as the appointment of Chief Artificial Intelligence Officers, is a step in the right direction. The Commission recommends that those CAIOs develop and incentivize the adoption of national training standards for individuals who review and analyze FRT algorithm results before those results are shared with investigators or other stakeholders. For FRT that is rights-impacting, CAIOs should 1) asses the AI in a real-world context to determine whether the FRT model results in significant disparities in the model's performance across demographic groups, 2) mitigate disparities that lead to, or perpetuate, unlawful discrimination and harmful bias, and 3) consult affected communities to solicit feedback in the design, development, and use of FRT, using this feedback to inform departmental decision making regarding FRT.

CAIOs should also consult DHS's Maryland Test Facility as a template for the "Build Once, Use Widely" approach to FRT testing to ensure the FRT will work in its intended real-world contexts.

Departmental Transparency & Oversight Actions. Departments should post on their public-facing websites whether they use FRT and whether training is required prior to such use. If it uses FRT, a department should have a publicly available use policy. It should audit its FRT use

[774] Pg. 93
[775] Pg. 31

and ensure it complies with government policy and should support research to improve accuracy and minimize demographic biases of current and potential FRT uses.

To cultivate greater community trust, departments should adopt more inclusive designs and engage with communities to help individuals understand the technology's capabilities, limitations, and risks. Disclosure and consent requirements are insufficient in providing consumers agency over their data used in air travel and housing decisions. In addition to adequate privacy protections, consumers should be able to consent to how, where, when, and under what circumstances their personal data will be utilized.

To support their CAIOs, departments should enable close coordination between CAIOs and existing responsible officials and organizations within their departments, including the Civil Rights and General Counsel offices, to advise and update departmental FRT guidance, implementation, and oversight.

Departmental Procurement Actions. Departments should require that all FRT procured by the federal government meets NIST's minimum accuracy level. FRT vendors should provide law enforcement agency users with ongoing training, technical support, and software updates needed to ensure their FRT systems can maintain high accuracy across demographic groups in real-world deployment contexts.

Federal Grantee Actions. Recipients of federal grants across DOJ, DHS, and HUD should be required to meet several accuracy, equitability, and due diligence standards with regard to their use of federally funded FRT:

- Grantees should provide verified results with respect to accuracy and performance across demographics from NIST's Facial Recognition Technology Evaluation, or a similar government-validated third-party test.
- FRT should be only part of a multi-factor basis for an arrest or investigation, in line with current fact-sensitive determinations of probable cause and reasonable suspicion.
- Grantees should adopt policies to disclose to criminal suspects, their lawyers, and judges on a timely basis the role FRT played in law enforcement actions, such as lead identification, investigative detention, the establishment of probable cause, and arrest.
- Grantees should disclose to suspects and their lawyers, on arrest and in any subsequent charging document, that FRT was used as an element of the investigation that led to the arrest and specify which FRT product was used.

With the publication of this report, including its findings and recommendations, the U.S. Commission on Civil Rights brings a crucial civil rights perspective to the nation's discussion on responsible federal use of FRT. The bipartisan effort and support that made this report possible indicates that there is a very real opportunity for the United States Government to meet this

moment of immense technological potential with due consideration and protections for the civil rights of every American.

[This page is left intentionally blank]

Statement of Commissioner Magpantay

Artificial intelligence (AI) and facial recognition technology (FRT) have sparked controversy due to its potential threats to civil liberties and privacy. The concerns are bipartisan.[776] Democrats are worried about FRT's unregulated use by law enforcement and its ingrained biases. Republicans are troubled by the potential for government to overuse FRT and the creation of an over-surveilled society that stifles personal freedoms.

With the foresight of Commissioner Mondaire Jones, the U.S. Commission on Civil Rights investigated the civil rights implications of the federal use of FRT. Subject-matter experts, FRT vendors, federal officials, and civil rights advocates explained FRT's utilization across multiple federal agencies, how FRT works, and provided examples of when FRT has both exonerated and wrongly incarcerated individuals.

From these experts, we also learned about how one-to-many matching leads to false matches. African Americans and Asian American, Native Hawaiian, and Pacific Islanders are subjected to significantly higher false positive rates of 10 to 100 times more than white individuals.[777] In one famous 2018 study, researchers found that several commercial algorithms that were used to classify individuals by race and sex exhibited error rates between 0.8% for light-skinned males, and 35% for dark skinned-females.[778]

However, present-day FRT algorithms have drastically improved in accuracy. Many of the top 100 algorithms ranked by the National Institute of Standards and Technology (NIST) today have less than a 1% error rate across all demographics. In 2020, the Director of the Information Technology Laboratory for NIST, Dr. Charles Romine testified before the U.S. Homeland Security Committee that with the highest-performing algorithms they saw "undetectable" bias, further noting, that they did not see a "statistical level of significance" related to bias in these top-performing algorithms.[779]

Still, faulty FRT has resulted in wrongful arrests of innocent people.[780] Harvey Eugene Murphy, Jr., Michael Oliver, Najeer Parks, Randal "Quaran" Reid, Alonzo Sawyer, Robert Williams, and Porcha Woodruff—these are the names of innocent individuals who were wrongly arrested due to misidentification by FRT. Faulty FRT is employed in various federal and state agencies, subjecting

---

[776] Drew Harwell, *Both Democrats and Republicans blast facial-recognition technology in a rare bipartisan moment*, The Washington Post (May 22, 2019), https://www.washingtonpost.com/technology/2019/05/22/blasting-facial-recognition-technology-lawmakers-urge-regulation-before-it-gets-out-control/.
[777] Patrick Grother, et al., Face Recognition Vendor Test (FRVT), NIST (Dec. 2019), nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[778] Buolamwini, J. and Gebru, T., Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research 81:1–15, 2018 Conference on Fairness, Accountability, and Transparency (Feb. 4, 2018), https://www.media.mit.edu/publications/gender-shades-intersectional-accuracy-disparities-in-commercial-gender-classification/.
[779] John Wagner, Facial Recognition and Biometric Technology, C-SPAN (Feb. 6, 2020), https://www.c-span.org/video/?469047-1/facial-recognition-biometric-technology.
[780] Robert Williams, *I Did Nothing Wrong. I Was Arrested Anyway.*, ACLU (July 15, 2021), https://www.aclu.org/news/privacy-technology/i-did-nothing-wrong-i-was-arrested-anyway.

Americans to potential civil rights and civil liberties violations. While FRT can be accurate at high-rates, one misidentification can destroy someone's life and traumatize an entire community.

I am also troubled by the widespread use of FRT throughout society and the lack of options for American citizens to opt-out of the technology. While traveling through the airport to attend this report's briefing, I observed challenges in identifying non-facial recognition security options at the Transportation Security Administration (TSA) checkpoints, despite their mandated availability. The required signage for alternative screening methods was neither conspicuous nor easily located. I brought this concern to the attention of TSA officials during our briefing. Furthermore, I noted that the existing signs appeared to be predominantly in English, potentially limiting accessibility for non-English speaking travelers. It is concerning to know that the millions of travelers using airports across the United States every day are subjected to mandatory FRT without a clear opt-out mechanism.

During this report's briefing, we learned about instances that FRT was useful. For example, the Department of Homeland Security (DHS) used Clearview AI to identify a man in a sexually explicit video involving a minor.[781] The technology scraped countless publicly available web images which allowed investigators to match it to Scott Barker's Facebook profile. DHS investigated Barker, found further connections between Barker and the child in the video, and was able to arrest Barker within two weeks. DHS has used FRT to help identify hundreds of perpetrators of child exploitation.

Yet, critics[782] argue that Clearview AI collected billions of social media images without user consent and provided them to law enforcement, effectively placing individuals in a "perpetual police line-up."[783] While this raises significant concerns, I commend Clearview AI's Founder, Hoan Ton-That, for appearing before the Commission during our briefing. It is pertinent that the Commission hears from industry leaders as we develop our report to understand the impact of FRT use on civil rights. I appreciate Clearview AI's willingness to engage with the federal government and address our questions.

Similarly, I commend DHS for participating in the Commission's briefing as well. We appreciate DHS's willingness to engage with us as we investigate this important civil rights issue. I also

[781] Thomas Brewster, *Exclusive: DHS Used Clearview AI Facial Recognition in Thousands of Child Exploitation Cold Cases*, Forbes (Aug. 7, 2023), https://www.forbes.com/sites/thomasbrewster/2023/08/07/dhs-ai-facial-recognition-solving-child-exploitation-cold-cases/?sh=4c07cff97682.
[782] Kashmir Hill, *Clearview AI, Used by Police to Find Criminals, is Now in Public Defenders' Hands,* The New York Times (June 21, 2023), https://www.nytimes.com/2022/09/18/technology/facial-recognition-clearview-ai.html.
[783] Katherine Tangalakis-Lippert, *Clearview AI scraped 30 billion images from Facebook and other social media sites and gave them to cops: it puts everyone into a 'perpetual police line-up'*, Business Insider (Apr. 2, 2023) https://www.businessinsider.com/clearview-scraped-30-billion-images-facebook-police-facial-recogntion-database-2023-4.

acknowledge DHS's proactive steps in developing guardrails and clear policies to address civil rights concerns related to its FRT use, particularly through the DHS Directive.[784]

I applaud Congressional leaders in its current search for bipartisan solutions:

- **Senate Majority Leader Chuck Schumer** (D-NY) organized bipartisan Senate Forums over the past year to educate senators on how AI works.[785]
- **Speaker Mike Johnson** (R-LA) and **Democratic Leader Hakeem Jeffries** (D-NY) established a bipartisan House Task Force on AI earlier this year to explore how Congress can ensure innovation while considering guardrails.[786]
- **Senators John Kennedy** (R-LA) and **Jeff Merkley** (D-OR) have introduced bipartisan legislation to end involuntary facial recognition screening at airports.[787]
- **Rep. Ted Lieu** (D-CA) has introduced multiple bills curbing law enforcement's use of FRT.[788]
- **Rep. Mark Meadows** (R-NC) has urged for federal laws to restrain FRT use before "it gets out of control."[789]
- **Senators Mike Rounds, Martin Heinrich, Todd Young** who are serving on the Senate Bipartisan Working Group on AI
- **Reps. Jay Obernolte and Ted Lieu**, who are serving as chair and co-chair, respectively, of the House Task Force on Artificial Intelligence

Last year, the White House directed[790] federal agencies to set standards for AI safety and security with an AI Bill of Rights.[791] This year, the Office of Management and Budget issued its first AI

[784] Use of Facial Recognition and Face Capture Technologies, Department of Homeland Security (Sept. 11, 2023), https://www.dhs.gov/sites/default/files/2023-09/23_0913_mgmt_026-11-use-face-recognition-face-capture-technologies.pdf.
[785] Statement from the Eight Bipartisan Senate Forum on Artificial Intelligence, Senator Chuck Schumer (Dec. 6, 2023), https://www.schumer.senate.gov/newsroom/press-releases/statements-from-the-eighth-bipartisan-senate-forum-on-artificial-intelligence.
[786] House Launches Bipartisan Task Force on Artificial Intelligence, Rep. Hakeem Jeffries (Feb. 20, 2024), https://democraticleader.house.gov/media/press-releases/house-launches-bipartisan-task-force-artificial-intelligence.
[787] Lauren Sforza, *Senators introduce bipartisan legislation ending involuntary facial recognition screening,* The Hill (Nov. 29, 2023), https://thehill.com/policy/technology/4333664-senators-legislation-facial-recognition-screening/.
[788] Reps Lieu, Jackson Lee, Clarke, Gomez, Ivey, and Veasey Introduce Bill to Regulate Law Enforcement's Use of Facial Recognition Technology, Rep. Ted Lieu (Oct. 27, 2023), https://lieu.house.gov/media-center/press-releases/reps-lieu-jackson-lee-clarke-gomez-ivey-and-veasey-introduce-bill.
[789] Harwell, *supra* note 1.
[790] FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, The White House (Oct. 30, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.
[791] Blueprint for an AI Bill of Rights, Office of Science and Technology Policy (Oct. 4, 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

government-wide policy,[792] requiring all federal agencies to implement AI safeguards. DHS's Office of Civil Rights & Civil Liberties has been proactive in instituting protections in its use of FRT.[793]

Experts and advocates agree that regulators need to wholly understand the reality of AI and FRT. Bipartisan legislation should:

(1) establish guardrails for law enforcement's use of FRT, requiring multiple conditions before utilization for an investigation, such as mandating a minimum level of image quality, conducting multiple blind peer reviews of potential matches, and using a possible match as only an investigative lead and not as sole grounds for probable cause;

(2) require FRT developers and deployers to undergo regular bias mitigation training and consistently evaluate and monitor FRT to minimize racially disparate matching error rates;

(3) ensure transparent documentation of legal compliance efforts undertaken and steps taken to prevent discrimination;

(4) provide public-facing explicit notice and communication of FRT's use of individuals so they can be informed when their images are subject to an FRT search;

(5) provide clear and noticeable opt-out mechanisms to individuals whenever facial and biometric data is being collected, processed, or analyzed by FRT;

(6) create accountability by establishing a standard of due diligence for FRT providers and a system of redress, such as a private right of action, for those who have been wrongly identified and wrongly detained in bad facial matches.

(7) require a minimum accuracy level of 98% across all demographics according to NIST testing for an algorithm to be deployed into the real world.

Public policy has always lagged behind technological innovation. However, the consequences are too severe to wait any longer. Our civil liberties and civil rights are at stake.

It is time for Congress to act on artificial intelligence and facial recognition technology.

---

[792] FACT SHEET: Vice President Harris Announces OMB Policy to Advance Governance, Innovation, and Risk Management in Federal Agencies' Use of Artificial Intelligence, The White House (Mar. 28, 2024), https://www.whitehouse.gov/briefing-room/statements-releases/2024/03/28/fact-sheet-vice-president-harris-announces-omb-policy-to-advance-governance-innovation-and-risk-management-in-federal-agencies-use-of-artificial-intelligence/.

[793] *Supra* note 784.