**STATEMENT OF NICOL TURNER LEE**

**Senior Fellow, Governance Studies and**

**Director, Center for Technology Innovation,**

**The Brookings Institution**

**Before the United States Commission on Civil Rights**

**Public Briefing: “Civil Rights Implication of the Federal Use of Facial Recognition Technology”**

**March 8, 2024**

Chair Garza, Vice Chair Bourse, and distinguished members of the United States Commission on Civil Rights, thank you for the invitation to testify on the important issue on the federal use of facial recognition technology (FRT). I am Nicol Turner Lee, Senior Fellow in Governance Studies, and Director of the Center for Technology Innovation at the Brookings Institution. With a history of over 100 years, Brookings is committed to evidence-based, nonpartisan research in a range of focus areas. My research expertise encompasses data collection and analysis around regulatory and legislative policies that govern telecommunications and high-tech industries, along with the impacts of digital exclusion, artificial intelligence, and machine learning algorithms on vulnerable populations. My forthcoming book, *Digitally Invisible: How the Internet Is Creating the New Underclass* will be published by Brookings Press later this summer.

I have spent the last few months as a member of the National Academies’ appointed research commission on the use of facial recognition, which was sponsored by the United States Department of Homeland Security (DHS, and the Federal Bureau of Investigations (FBI). The committee’s final report, titled “Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance,” was published in January 2024 and offers a series of technical explanations, challenges, and recommendations at a time when facial recognition is increasingly being used in law enforcement investigations.[[1]](#footnote-2) As expected, concerns around equity, privacy, and the protection of existing civil rights emerged as critical themes in the report, as well as the need to think about future use cases of facial recognition by federal agencies and other police entities, including Customs and Border Patrol.

In my testimony, I want to reinforce many of the recommendations of that report, particularly those that speak to reasonable and equitable standards when it comes to facial recognition use, and specific calls to federal legislators to consider the risks, outcomes, and best practices that certify the use of the technology and offer greater transparency. I also propose in this statement that the federal government ‘lead by example’ by having reasonable requirements for procuring and using such technology and doing so in a way that respects the data privacy of individuals and their communities. Finally, 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 Attorneys General, 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.

The federal government, which has authority and oversight over massive amounts of public data, must act both ethically and responsibly in its use of facial recognition. And it must do so in ways that either enact appropriate guardrails over FRT, or decide to not to use it all, especially when the equity stakes are high. I will close my testimony with suggested recommendations that the Commission can consider when evaluating how the government can act responsibly in FRT adoption and use.

**II.** **Defining facial recognition technologies**

Even before Eadweard Muybridge captured the first ever motion picture of a Black man riding a horse in 1887, the history of photography and the history of Black people in America have been intertwined.[[2]](#footnote-3) Pioneering Black photographers and abolitionists like Glenalvin Goodridge and James Pressley Ball sought to document the cruelties of slavery, and famed intellectual Frederick Douglass would become the most photographed American of the 19th century.[[3]](#footnote-4) Nonetheless, the history of photography’s technical development has often been a history of the erasure of Black people. Before the advent of digital technology, photography involved exposing photo-sensitive materials to light and then chemically processing those materials to develop an image. The degree of contrast in the resulting images was determined by the photographic techniques and the composition of the chemicals used in film processing. Initially, photography was only accessible to wealthy white families, so early photographs used stark contrast that could capture the appearances of people with light skin but left those with dark skin virtually indistinguishable. Photographic techniques that were able to document Black people at all were only invented to capture images of furniture and even horses with darker textures.[[4]](#footnote-5)

Beginning in 1954, Kodak used Shirley Cards—images of a white Kodak employee named Shirley—to calibrate their film production.[[5]](#footnote-6) As color printing became more accessible, Kodak and other film manufacturers began sending these cards to print businesses, meaning that virtually every machine in the printing industry was specifically calibrated to render images of white women, resulting in poorly rendered images of Black people. In the 1950s and 1960s, Kodak largely ignored complaints from Black parents that their children were visually obscured in school photographs.[[6]](#footnote-7) The company only improved the ability of their film to capture darker hues in the 1970s, after lobbying from furniture makers and chocolate manufacturers,[[7]](#footnote-8) and Kodak did not produce a multiracial Shirley Card until the mid-90s.[[8]](#footnote-9) Although the digital photography technology now used in surveillance cameras worldwide works differently, similar problems persist, and photographic methods still perform poorly for people with darker-skinned complexions, and equipment failures, like low quality cameras or poorly lit settings, contribute to poor quality images and, thus, false results for Black people in FRT systems.

Although the field of AI has existed for nearly 70 years, only in the past decade has the automated identification of facial images become technically feasible. Today, AI is based on the paradigm of machine learning, in which computers learn complex patterns from large amounts of “training data” to make predictions, such as whether two facial images can be easily detected and matched. Because these training data are the material from which the system learns, any human biases that exist in the training data will also be learned by the system, and poorly represented datasets can essentially direct the design and findings of AI systems. Extensive documentation already exists on the demographic biases in AI systems that are contributing to unfair outcomes in critical quality-of-life sectors, including banking, housing, employment, education, healthcare, policing, and prison sentencing.

Facial recognition systems work by analyzing photographic data in the form of a grid of pixels, “rows and columns of numbers indicating intensities of color and brightness,” and determining which patterns of numerical values indicate facial characteristics.[[9]](#footnote-10) To compare an image of one face against another, a facial recognition system must transform the image into a comparable “template,” a numerical expression that represents the basic facial characteristics in such a way that they can be reliably compared against a template derived from another image.[[10]](#footnote-11) Facial recognition systems derive these templates by passing an image through “filters,” which manipulate pixel values to derive a facial template; facial recognition systems often pass an image through multiple filters to derive a template, or “fingerprint.”[[11]](#footnote-12)

Developing filters that reliably derive accurate templates involves a process of trial and error—this can be automated using deep learning, which trains the system to produce reliable filters on large datasets of images.[[12]](#footnote-13) The more images that a model can be trained on, the more accurate it will be. That is because facial recognition systems need to be trained on certain facial characteristics to be able to recognize them and develop filters which will reliably incorporate them into the image template. If a facial recognition model’s training data does not include any images of people who are missing an eye, for example, then its filters may fail to develop accurate templates for images of those individuals if they are later passed into the system, which would lead to the system being less accurate in identifying and matching those individuals faces. Likewise, when a facial recognition system is trained on a set of photos that are primarily white and male, the system will be better at matching white male faces, and worse at matching black female faces.[[13]](#footnote-14)

The National Institute for Standards and Technology’s (NIST) Face Recognition Vendor Test has found that FRT algorithms are less accurate when used to identify women and people of color.[[14]](#footnote-15) The FRVT did find that this bias is sometimes much lower in the most accurate algorithms, which one test found returned the wrong image less than 0.1% of the time.[[15]](#footnote-16) However, this low error rate is highly dependent on numerous factors, including the algorithm, quality of the query image, and the size of the search database. The best algorithms are extremely accurate when trying to find a match for a high-quality image while searching a standardized database—such as a database of driver’s license photos—but they are far less accurate when analyzing lower quality images. When analyzing live video, error rates are much higher, varying between 13% and 64%.[[16]](#footnote-17) When error rates are higher, bias becomes more pronounced.[[17]](#footnote-18)

This leads to another serious concern of FRT, which is its broad and often ambiguous use by law enforcement, which is often done without the appropriate training or clear guidance on the contexts and circumstances for which it should be permitted. In fact, it is often unknown when law enforcement agencies are using FRT for investigations and surveillance because there is no external notification. The extreme lack of transparency is a serious issue, because the context in which FRT is used greatly impacts how effective—and thus how biased—it is. In fact, a recent report from Georgetown University referred to FRT as a “forensic without a science.”[[18]](#footnote-19)

Nevertheless, and in spite of “widespread consensus across police departments… that a face recognition match is an investigative lead only and does not by itself amount to probable cause to make an arrest,” there are multiple documented instances of FRT being used as the sole basis for an arrest; the “systemic lack of transparency” regarding law enforcement’s use of makes it impossible to determine how often this happens.[[19]](#footnote-20) FRT is an unproven technology for its use in law enforcement, and its application in this context creates a number of issues for its accuracy and equity.

To date, six people are known to have been falsely arrested due to an incorrect FRT match, all of whom are Black; their cases will be detailed in the next section.[[20]](#footnote-21) The real number might be higher. What these racially motivated arrests by FRT do indicate is that a combination of technical failures and, even more importantly, procedural failures in which investigators used the technology irresponsibly or failed to act as a crucial “human in the loop” could be likely culprits. Without standards and best practices for the use of FRT by law enforcement, as well as transparency on it is used, law enforcement agencies’ use of FRT are using the technology must be continuously studied and evaluated to determine the efficacy of its use as a forensic tool. Without this intervention, FRT will continue to perpetuate racial biases and continue our history of oversurveillance of people of color.

**III. Facial recognition and the invasion of civil rights**

*The cases of false arrests*

In 2019, a teacher called Detroit Police after witnessing a fight between students. After the teacher recorded the incident on his phone, one of the students reached into the teacher’s vehicle and threw his phone, cracking the screen and breaking the case. The Detroit Police uploaded footage from the incident into a facial recognition system, which identified Michael Oliver, a 25-year-old Black man, as a lead suspect. The teacher then identified Oliver in a photo lineup. Consequently, Oliver was charged with a felony count of larceny, but Oliver had tattoos that the man in the video clearly did not. After the prosecutor and teacher reviewed the footage and confirmed that there was a misidentification, the case was dismissed. While the Wayne County Prosecutor’s Office now has more stringent protocol for facial recognition technology cases, Oliver’s case makes clear the direct harm FRT misidentification can cause.[[21]](#footnote-22)

Also in 2019, after a suspected shoplifter in Woodbridge, New Jersey allegedly hit a parked police car with his own vehicle after police officers noticed his license was fraudulent, a detective in the Woodbridge Police Department sent the photo from the fake driver’s license to state agencies with access to FRT. State investigators reported that their system had matched the photo to a license photo of 33-year-old Nijeer Parks. The Woodbridge detective agreed the photo matched the fake license, and police issued a warrant for Parks’ arrest. However, when the crimes were committed, Parks was at a Western Union 30 miles away. He had a photograph of his receipt corroborating his story, but Parks was still jailed for at least 10 days and, facing years behind bars were he to be convicted, spent around $5,000 for legal defense. It took nine months for his case to be dismissed for lack of evidence.[[22]](#footnote-23)

In 2020, Detroit Police were searching for a suspect who stole five watches from a Shinola retail store. Detectives uploaded an image from the store’s security footage to a FRT system, which returned an image of Robert Julian-Borchack Williams, a 42-year-old Black man in Farmington Hills, Michigan, as one of multiple possible matches. The store’s loss-prevention contractor, who did not personally witness the crime, then identified Williams from a lineup of six photographs. Police went to Williams’ home and arrested him while he stood on his front lawn in front of his wife and two daughters, ages 2 and 5, who cried as they watched their father being taken away. Williams was held overnight. Around noon the next day, Williams demonstrated to detectives that he was clearly not the same person as the man in the surveillance footage; he remained in custody until that evening, for a total of 30 hours overall. At his scheduled hearing, a Wayne County prosecutor dropped the charges against Williams due to insufficient evidence.[[23]](#footnote-24)

In 2022, Louisiana authorities jailed 22-year-old Randall Reid after FRT misidentified Reid as a suspect for the theft of $10,000 worth of luxury purses in a New Orleans suburb. However, because Reid had never been to Louisiana. Reid’s attorney said he was falsely linked to the purse theft. Cosmetic differences, such as a mole on Reid’s face, forced the authorities to rescind the warrant and release him from jail after five days of confinement. This came after the New Orleans City Council had previously voted to allow law enforcement to use FRT leads generation.[[24]](#footnote-25)

Alonzo Sawyer spent nine days in confinement in 2022 after law enforcement alleged that he had assaulted a bus driver near Baltimore and stole their smartphone. Intelligence analysts had employed FRT to label Sawyer as a possible match. Sawyer’s wife protested, drawing attention to differences between Sawyer and the suspect, including differences in height, age, facial hair, and walking patterns. Law enforcement later identified another suspect. He was seven inches shorter and twenty years younger than Sawyer. Sawyer’s case, among many others, highlights the risk law enforcement runs when confining people and harming their reputations based on faulty technology.[[25]](#footnote-26)

In February 2023, Porcha Woodruff, one of the only known women falsely accused, was wrongly accused of robbery and larceny after an outdated photo processed by FRT identified her as a match for Detroit police.[[26]](#footnote-27) She was arrested at her home before her children were headed to school, and most glaringly obvious was that she was also pregnant. The suspect in the grainy photo was not. Ms. Woodruff is now suing the city of Detroit after spending time at the station, and monies to prove her innocence. These costs do not include the trauma of her children who witnessed the interaction.

Each of these individuals, falsely arrested using FRT, are Black people, whose stories have been slowly made public in the last couple of years. And the fact that all these individuals are of a certain race also highlights the disproportionate risk of misidentification that Black people face from FRT, and the serious consequences that they faced after the fact. Faulty police procedures are largely to blame, and the way investigators utilized FRT in the above examples—not having a supervisor sign off on the match, presenting the matches in a lineup to someone who was not an eyewitness, or going forward with an arrest without any corroborating evidence—also leaves much to be desired. But even if the policies were improved, a framework that elevates the need equity in the design, use, and evaluation FRT is sorely needed.

While FRT systems are more accurate than ever before, their accuracy is highly dependent on the context of their use, and the consequences of their inaccuracy are disproportionately borne by marginalized communities. A framework for equity in the development and application of facial recognition technologies must focus on the system and policy design, training data, implementation, and outcome of facial recognition systems. Equity should also be thought of as fairness—more specifically, the “property of fairness of a decision-making agent”—although this definition remains imprecise.[[27]](#footnote-28) Insofar as an algorithm is fundamentally a decision-making agent, it is easy to see how the concept of equity extends to algorithms generally—and AI specifically—and to outline how algorithms might fail to account for or even perpetuate inequity. Further, equity should also defer to who is accounted for in federal, and local databases that are the reference for matches emanating from FRT. That is because what is driving these dissimilarities, or overfitting for technical accuracies is the disproportionate representation in the training sets, which was referenced earlier. As police departments and other law enforcement agencies use FRT to identify individuals who are stopped or arrested, the Center on Privacy & Technology at Georgetown Law found that, as of 2016, “one in two American adults is in a law enforcement face recognition network.”[[28]](#footnote-29) Due to a range of privacy and civil liberties concerns, getting the consent of more individuals to be subjected to photo capture systems outside of law enforcement and in more public and commercial settings is problematic, even in the era of greater surveillance on government-controlled grounds, like subway or bus stations. Here, the intended purposes for that data collection must still be transparent to users. For example, someone sitting on a public transportation platform may believe that they are being filmed for public safety, while a person who is booked for a crime implicitly consents to engagement in a wider criminal database.

In sum, law enforcement agencies must acknowledge the systemic problems associated with FRT use and dissemination at all stages. And there are clearly other cases for consideration that the Commission consider as it determines the legalities and fate of FRT.

IV. **Harms in other use cases outside of policing**

A breadth of sectors now implements FRT in some way. In June 2021, the IRS signed a two-year contract worth $86 million with ID.me to authenticate online accounts using FRT.[[29]](#footnote-30) This decision proved controversial, as many unemployment applicants reported that the FRT model failed to properly identify them, locking them out of unemployment benefits and putting their physical and financial wellbeing in jeopardy.[[30]](#footnote-31) The use of FRT is not restricted to the contexts of hiring, government benefits, and law enforcement, but it is rather increasingly being deployed across a wide variety of sectors, creating many unique equity challenges. FRT models are being developed for and advertised to schools, both as a security measure and as an educational tool designed to monitor students’ engagement and development.[[31]](#footnote-32)

Among students, the use of the technology poses various risks for children, including stigmatizing youth who develop differently, causing long lasting psychological harms due to surveillance, and reinforcing existing inequities in education by misidentifying students of color.[[32]](#footnote-33) The Center for Democracy and Technology found that, in some instances, FRT was being installed on student-issued laptops, and enabled as ‘back doors’ to disciplinary action – justified and unjustified.[[33]](#footnote-34)

FRT is also being deployed in the healthcare sector, where it has been used to diagnose genetic, medical, and behavioral conditions, as well as to monitor patients to predict behavior, pain, and emotion.[[34]](#footnote-35) The financial services industry has also been implementing the technology, with banks using FRT both to verify users’ identities when accessing their accounts and even to develop facial-recognition payment systems, wherein a user can make a payment at a retail location simply by allowing their face to be scanned by a camera.[[35]](#footnote-36) The increasing prevalence of FRT must raise equity concerns regarding its aforementioned problems with accuracy in terms of race and gender, as well as regarding accessibility for the visually impaired.[[36]](#footnote-37)

In addition to sectoral claims on the technology, the increased use of surveillance technology is also a compromise on civil liberties. In a 2020 article, Chaz Arnett traces the evolution of “racialized surveillance” of Black people in America from “the first iterations of policing through slave patrols,” through their evolution into frequent arrests immediately after emancipation, and to the intensification of “surveillance of Black communities, organizations, reporters, and leaders” during the civil rights movement.[[37]](#footnote-38) Surveillance of Black civil rights leaders during this latter period was executed on a national scale, organized by the FBI’s “Racial Matters” and COINTELPRO programs.[[38]](#footnote-39) Arnett uses the city of Baltimore as a lens to examine how this history has continued into the present-day, describing, as an example, how 90 percent of the Baltimore police’s use of “StingRay” phone-tracking technology occurred “in majority non-white Census block groups, where residents are overwhelmingly Black.”[[39]](#footnote-40)

A wide variety of other marginalized communities have historically been subjected to oversurveillance, and intersectional identities can multiply these risks. For example, in the wake of the September 11th attacks, Muslim and South-Asian communities have come under invasive surveillance from both federal and local law enforcement authorities. Additionally, Hispanic communities are frequently surveilled by immigration enforcement authorities.[[40]](#footnote-41) In a 2011 article, Rachel L. Flin documents these dynamics:

In the USA, while black men experience disproportionate levels of surveillance in relation to the politics of crime, in relation to citizenship, Spanish speaking peoples of Mexican, Central or South American origin or descent are often constructed as potentially illegal immigrants and subject to heightened border or employment surveillance. In contrast, those of South Asian or Middle Eastern origin or descent are constructed as potential ‘terrorists’ and experience disproportionate surveillance on transport and at borders.[[41]](#footnote-42)

 Compounding all these systems of oversurveillance is surveillance based on class. Surveillance disproportionately falls on poor Americans, who themselves are disproportionately women and people of color—the same populations for whom, it must be noted, FRT is least effective.[[42]](#footnote-43) In a 2012 article, Michele Estrin Gilman documents how poor Americans “endure a barrage of information-collection practices that are far more invasive and degrading than those experienced by their far wealthier neighbors.”[[43]](#footnote-44) This surveillance is often connected with enrollment in welfare practices, which can involve requirements to submit to “drug tests or finger imaging or unsolicited family-planning advice, such as pressure to implant a Norplant birth control device.”[[44]](#footnote-45) In terms of employment, poor Americans are also concentrated in service-industry jobs, which often involve “visible—sometimes humiliating—surveillance tactics such as psychological testing, regular screening, and overt videotape monitoring.”[[45]](#footnote-46)

 Taken together or apart, these use cases suggest a significant risk that FRT could be weaponized by law enforcement and a host of other actors as one more component of an arsenal disproportionately brought to bear against marginalized communities.

*Private companies and FRT procurements systems*

The private designers of these biometric FRT systems often coordinate with federal, state, and local law enforcement agencies. Clearview AI is one of the more prominent commercial providers of FRT to law enforcement agencies.[[46]](#footnote-47) The private start-up has scraped billions of publicly available images and, as of 2021, partnered with over 3,100 federal and local law enforcement agencies to identify people outside the scope of government databases.[[47]](#footnote-48) While the FBI only has about 640 million photos in its databases, Clearview AI has about 10 billion.[[48]](#footnote-49)

 In January 2021, the Biden administration issued an executive order directing federal agencies to conduct equity assessments to review any obstacles that marginalized communities, including individuals of color, encounter when trying to access to government resources and services.[[49]](#footnote-50) Brookings Institution Nonresident Senior Fellow Mark MacCarthy has argued that the U.S. should adopt a system for prior assessments of facial recognition systems in law enforcement.[[50]](#footnote-51) Vendors in the U.S. have tried to respond to these concerns by publicly supporting bills that would allow government agencies to use facial recognition with restrictions designed to ensure it was not deployed for broad surveillance purposes.[[51]](#footnote-52)

Over the last several years, the NIST has established criteria for evaluating the accuracy and fairness of FRT and has published independent assessments of vendor systems that have been voluntarily submitted to them for evaluation.[[52]](#footnote-53) These tests include various measurements, including ensuring a particular accuracy rate. However, there are limitations to these tests. Some analysts suggest that merely undergoing NIST assessment is too low a bar to justify deploying such significant FRT systems. Moreover, despite several years of research, there is still no agreed upon definition of algorithmic fairness.[[53]](#footnote-54) While experts of demographic fairness and biometric systems contend that standardized evaluation metrics should be developed and applied to measure and compare bias in a transparent manner, this lack of consensus complicates system-wide efforts.[[54]](#footnote-55)

To date, there is simply no scientific basis establishing FRT’s reliability as a forensic tool, and on face value, the intentions of its use in other use cases should be scrutinized without more research.

**VI. Recommendations**

The federal government can take immediate and long-term steps to prevent some of the systemic and more common-sense mistakes that happen when FRT is not properly used or contextualized. As “the reliability of face recognition as applied [as a forensic tool] has not been established,” robust scientific research of all possible components of the law enforcement FRT use process is imperative.[[55]](#footnote-56) Without such research, determining the accuracy of FRT’s use by law enforcement will be impossible. Thus, the federal government must aggressively establish a research agenda around some of the recommendations from the National Academies report which require additional data to validate FRT’s effectiveness. The fact-finding happening at the U.S. Civil Rights Commission should be additive to more formal research being developed on the technical cadence of modern-day FRT, as well as more sociological and legal inquiries into the technology’s value in a highly unequal society. Further, a broad research agenda should encompass increased and targeted appropriations to the National Academies and the National Science Foundation to gather data on the socio-technical implications of FRT design and deployment, and perhaps lead to more inclusive datasets that embolden greater technical accuracy. Research could also help to explain the implications of civil liberties and assess what equity really looks like in a society where surveillance is not equally applied to all people, especially those who have become citizen video patrollers with more available commercial video devices. What I’m suggesting is that the Commission expand its framing of the concern, even outside the scope of civil rights.

The federal government must also determine the most appropriate guardrails and guidance on FRT. Currently, congressional legislation is primarily limited to federal police, and other actors given the limited jurisdiction, oversight, and enforcement. As the government leads by example, using what they control as the basis for future legislation may not be a bad idea. Legislators have introduced both bans and limitations on FRT at the federal, state, and local levels, including the Traveler Privacy Protection Act, which ban TSA from using FRT in airports, a bill in the Massachusetts state legislature which would require a warrant for the use of FRT by law enforcement, and two bills in the Baltimore City Council which seek to impose data privacy requirements on the use of FRT.[[56]](#footnote-57) These bills, if enacted, may help frame how the technology is used more ethically and responsibly. Or, if this debate is left undone, they may also lead to outright bans.

Even with federal actions, much of FRT use has been driven at the local levels, including among local law enforcement agencies who are making decisions about its permissibility. There must be a radical improvement in law enforcement agencies’ transparency regarding FRT, including which systems they use, under which procedures and how often they use them, and how they proceed with the outcome of an FRT search. The current state of law enforcement’s use of FRT is incredibly opaque. Without an accurate assessment of how FRT is actually being used, ensuring equity in its use will be impossible. Furthermore, given the lack of empirical information about FRT’s accuracy as a forensic tool, the use of FRT must be considered evidence that the state is obligated to disclose to the defendant, who must be able to exercise their right to impeach unproven facial recognition systems as a witness.

These measures are necessary as first steps toward a more equitable framework for FRT use, but there are several other measures that will likely be necessary as well. There must be a national fair and equitable use standard for the use of FRT by law enforcement, which should include requirements for robust public disclosures. It should be emphasized that FRT may, if proven accurate in each context, be part of a suite of other investigative tools, but, even then, it may not always be necessary for use among law enforcement. FRT may also be prohibited for use in certain cases, either by private actors or in investigations of low-level or nonviolent offenses, to reduce the likelihood that a potentially risky tool is used unnecessarily and to limit the harms of oversurveillance. Furthermore, insofar as FRT is used by law enforcement, it must also be available to public defenders who can use the technology to gather potentially exonerating evidence.

Another point that the federal government should consider in FRT use by law enforcement and non-policing uses is retribution, and potential compensation, for those with observable and quantifiable harms. While more work needs to be done to assess the constitutionality of FRT in certain instances like mass surveillance, addressing the compliance with civil rights laws is only one part of the solution. The other part should focus on how we help individuals who have been wrongly accused by the technology and who are left without agency over an algorithmic decision. Right now, it is not clear who is responsible for the errors of machines and who pays when those who are falsely accused must cover the costs of lawyers, take off time from work, or address the post-traumatic stress of family members who are affected by the false arrest. Here is where the Commission, in partnership with the U.S. Department of Justice, could develop a fund for victims of FRT misidentification that led to an unjustifiable consequence which could impact future decisions, including the right to an unencumbered trial or the ability to access government services without a trace of one’s biometric consideration. My point is that companies and the federal government should not be indemnified from recourse when these systems go wrong.

In sum, acting on the proposed recommendations of the recent FRT report, developing a reasonable and equitable standard for FRT use and appropriate guardrails through best practices and/or legislation, and ensuring that impacted individuals have means for retribution and appeal are some of many recommendations before this Commission.

I thank you for the opportunity to testify and look forward to your questions. I am also grateful to Jack Malamud and Joshua Turner from Brookings for their assistance with this statement.

1. National Academies, “News Release: Advances in Facial Recognition Technology Have Outpaced Laws, Regulations; New Report Recommends Federal Government Take Action on Privacy, Equity, and Civil Liberties Concerns,” January 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 [↑](#footnote-ref-2)
2. Samantha Hill, “How Black people in the 19th century used photography as a tool for social change,” The Conversation, February 26, 2021, https://theconversation.com/how-black-people-in-the-19th-century-used-photography-as-a-tool-for-social-change-154721 [↑](#footnote-ref-3)
3. Michel Martin, “Picture This: Frederick Douglass Was The Most Photographed Man Of His Time,” NPR, December 13, 2015 https://www.npr.org/2015/12/13/459593474/picture-this-frederick-douglass-was-the-most-photographed-man-of-his-time [↑](#footnote-ref-4)
4. Damien Patrick Williams, “Fitting the description: historical and sociotechnical elements of facial recognition and anti-black surveillance,” Journal of Responsible Innovation, Vol. 7 No. S1, 2020 Mandalit del Barco, “How Kodak’s Shirley Cards Set Photography’s Skin-Tone Standard,” NPR, November 13, 2014, https://www.npr.org/2014/11/13/363517842/for-decades-kodak-s-shirley-cards-set-photography-s-skin-tone-standard [↑](#footnote-ref-5)
5. Mandalit del Barco, “How Kodak’s Shirley Cards Set Photography’s Skin-Tone Standard,” NPR, November 13, 2014, https://www.npr.org/2014/11/13/363517842/for-decades-kodak-s-shirley-cards-set-photography-s-skin-tone-standard [↑](#footnote-ref-6)
6. Ainissa Ramirez, “How 20th Century Camera Film Captured a Snapshot of American Bias,” Time, July 24, 2020, https://time.com/5871502/film-race-history/ [↑](#footnote-ref-7)
7. Sarah Lewis, “The Racial Bias Built into Photography,” The New York Times, April 25, 2019, https://www.nytimes.com/2019/04/25/lens/sarah-lewis-racial-bias-photography.html [↑](#footnote-ref-8)
8. Mandalit del Barco, “How Kodak’s Shirley Cards Set Photography’s Skin-Tone Standard,” NPR, November 13, 2014, https://www.npr.org/2014/11/13/363517842/for-decades-kodak-s-shirley-cards-set-photography-s-skin-tone-standard [↑](#footnote-ref-9)
9. David Leslie, “Understanding bias in facial recognition technologies,” *The Alan Turing Institute* (2020) https://www.turing.ac.uk/sites/default/files/2020-10/understanding\_bias\_in\_facial\_recognition\_technology.pdf [↑](#footnote-ref-10)
10. William Crumpler and James A. Lewis, “How Does Facial Recognition Work?” *CSIS* (June 2021) https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210610\_Crumpler\_Lewis\_FacialRecognition.pdf?VersionId=xdae\_qQa80\_Fimc1mzF3wxN6KIp.01Xg [↑](#footnote-ref-11)
11. Ibid. [↑](#footnote-ref-12)
12. Ibid. [↑](#footnote-ref-13)
13. Morgan Livingston, “Preventing Racial Bias in Federal AI,” Journal of Science Policy & Governance, May 2020 https://www.sciencepolicyjournal.org/uploads/5/4/3/4/5434385/livingston\_jspg\_v16.2.pdf [↑](#footnote-ref-14)
14. William Crumpler and James A. Lewis, “How Does Facial Recognition Work? A Primer,” CSIS, June 2021 https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210610\_Crumpler\_Lewis\_FacialRecognition.pdf?VersionId=xdae\_qQa80\_Fimc1mzF3wxN6KIp.01Xg [↑](#footnote-ref-15)
15. Ibid. [↑](#footnote-ref-16)
16. Ibid. [↑](#footnote-ref-17)
17. Ibid. [↑](#footnote-ref-18)
18. Clare Garvie, “A Forensic Without the Science: Face Recognition in U.S. Criminal

Investigations,” Center on Privacy & Technology at Georgetown Law, 2022 https://mcusercontent.com/672aa4fbde73b1a49df5cf61f/files/2c2dd6de-d325-335d-5d4e-84066159df71/Forensic\_Without\_the\_Science\_Face\_Recognition\_in\_U.S.\_Criminal\_Investigations.pdf [↑](#footnote-ref-19)
19. Ibid. [↑](#footnote-ref-20)
20. Katie Hawkinson, “In every reported case where police mistakenly arrested someone using facial recognition, that person has been Black,” Business Insider, August 6, 2023, https://www.businessinsider.com/in-every-reported-false-arrests-based-on-facial-recognition-that-person-has-been-black-2023-8 [↑](#footnote-ref-21)
21. Elisha Anderson, “Controversial Detroit facial recognition got him arrested for a crime he didn’t commit,” *Detroit Free Press* (10 July 2020) <https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/>; Natalie O’Neill, “Faulty Facial Recognition Led to His Arrest—Now He’s Suing,” *Vice* (4 September 2020) https://www.vice.com/en/article/bv8k8a/faulty-facial-recognition-led-to-his-arrestnow-hes-suing [↑](#footnote-ref-22)
22. Now, Mr. Parks is suing the police, the prosecutor, and the City of Woodbridge for false arrest, false imprisonment, and violation of his civil rights: John General and Jon Sarlin, “A false facial recognition match sent this innocent Black man to jail,” *CNN Business* (29 April 2021) <https://www.cnn.com/2021/04/29/tech/nijeer-parks-facial-recognition-police-arrest/index.html>; Kashmir Hill, “Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match,” *The New York Times* (29 December 2020) https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html [↑](#footnote-ref-23)
23. Kashmir Hill, “Wrongfully Accused by an Algorithm,” *The New York Times* (24 June 2020) <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>; Bobby Allyn, “’The Computer Got It Wrong’: How Facial Recognition Led To False Arrest Of Black Man,” *NPR* (24 June 2020) <https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig>; Jon Porter, “A black man was wrongfully arrested because of facial recognition,” *The Verge* (24 June 2020) https://www.theverge.com/2020/6/24/21301759/facial-recognition-detroit-police-wrongful-arrest-robert-williams-artificial-intelligence [↑](#footnote-ref-24)
24. The Associated Press, “Facial recognition tool led to mistaken arrest, lawyer says,” *The Hill* (2 January 2023) <https://thehill.com/homenews/ap/ap-u-s-news/ap-facial-recognition-tool-led-to-mistaken-arrest-lawyer-says/>; Thomas Germain, “Innocent Black Man Jailed After Facial Recognition Got It Wrong, His Lawyer Says,” *Gizmodo* (3 January 2023) https://gizmodo.com/facial-recognition-randall-reid-black-man-error-jail-1849944231 [↑](#footnote-ref-25)
25. Khari Johnson, “Face Recognition Software Led to His Arrest. It Was Dead Wrong,” *Wired* (28 February 2023) https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/ [↑](#footnote-ref-26)
26. Mirna Alsharif and Cristian Santana, “Detroit woman sues city after being falsely arrested while pregnant due to facial recognition technology”, NBC, August 6, 2023, https://www.nbcnews.com/news/us-news/detroit-woman-sues-city-falsely-arrested-8-months-pregnant-due-facial-rcna98447 [↑](#footnote-ref-27)
27. Emily Hadley, “Equity and Bias in Algorithms: A Discussion of the Landscape and Techniques for Practitioners,” *AMSTAT News* (1 September 2022) https://magazine.amstat.org/blog/2022/09/01/algorithms/. There are a multitude of possible definitions of fairness, many of which may be contradictory: Sahil Verma and Julia Rubin, “Fairness Definitions Explained,” *2018 ACM/IEEE International Workshop on Software Fairness* (29 May 2018) https://fairware.cs.umass.edu/papers/Verma.pdf. True fairness may be impossible in some scenarios. One research report focused on the COMPAS tool that judges use to assess the risk of recidivism in defendants divided fairness into three constituent properties—calibration within groups, balance for the negative class, and balance for the positive class—which it found were ultimately contradictory: Jon Kleinberg, Sendhil Mullainathan, and Manish Raghavan, “Inherent Trade-Offs in the Fair Determination of Risk Scores,” *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)* Article No. 43 (2017), pg. 43:1-43:23 https://drops.dagstuhl.de/opus/volltexte/2017/8156/pdf/LIPIcs-ITCS-2017-43.pdf. [↑](#footnote-ref-28)
28. Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, “The Perpetual Line-Up: Unregulated Police Face Recognition in America,” *Georgetown Law Center on Privacy & Technology* (18 October 2016) https://www.perpetuallineup.org/. [↑](#footnote-ref-29)
29. Alan Rappeport, “I.R.S. Will Allow Taxpayers to Forgo Facial Recognition Amid Blowback,” *The New York Times* (21 February 2022) https://www.nytimes.com/2022/02/21/us/politics/irs-facial-recognition.html [↑](#footnote-ref-30)
30. Todd Feathers, “Facial Recognition Failures Are Locking People Out of Unemployment Systems,” *Vice* (18 June 2021) https://www.vice.com/en/article/5dbywn/facial-recognition-failures-are-locking-people-out-of-unemployment-systems. As of January 2022, in addition to the IRS, ID.me worked with 27 states, multiple federal agencies, and hundreds of retailers: Joy Buolamwini, “The IRS Should Stop Using Facial Recognition,” *The Atlantic* (27 January 2022) https://www.theatlantic.com/ideas/archive/2022/01/irs-should-stop-using-facial-recognition/621386/. In February 2022, the IRS announced that individuals would be able to opt out of FRT by going through a live interview option, although some users encountered obstacles with this process as well: EPIC, “IRS Plan to Make Facial Recognition ‘Optional;’ Fails to Address Privacy and Equity Harms,” *Electronic Privacy Information Center* (22 February 2022) https://epic.org/irs-plan-to-make-facial-recognition-optional-fails-to-address-privacy-and-equity-harms/. ID.me initially claimed it did not use one-to-many identification—generally less accurate than one-to-one verification—before admitting that it did. As of February 2023, one year later, the IRS still has not released a roadmap for transitioning away from the exclusive use of ID.me Tonya Riley, “A year after outcry, IRS still doesn’t offer taxpayers alternative to ID.me,” *Cyberscoop* (9 February 2023) https://cyberscoop.com/irs-facial-recognition-identity-privacy/. [↑](#footnote-ref-31)
31. Ava Kofman, “Face Recognition Is Now Being Used In Schools, But It Won’t Stop Mass Shootings,” *The Intercept\_* (30 May 2018) https://theintercept.com/2018/05/30/face-recognition-schools-school-shootings/; Randy Rieland, “Can Facial Recognition Really Tell If a Kid Is Learning in Class?” *Smithsonian Magazine* (1 November 2013) https://www.smithsonianmag.com/innovation/can-facial-recognition-really-tell-if-a-kid-is-learning-in-class-8163550/#dcdIHLrADPjuCixb.99. [↑](#footnote-ref-32)
32. Nila Bala, “The Danger of Facial Recognition in Our Children’s Classrooms,” *Duke Law & Technology Review* Vol. 18 Iss. 1 (2019), pg. 249-267 https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1354&context=dltr [↑](#footnote-ref-33)
33. Kristin Woelfel, Ariana Aboulafia, and Elizabeth Laird, “Report – Late Applications: Protecting Students’ Civil Rights in the Digital Age,” Center for Democracy & Technology, September 20, 2023, https://cdt.org/insights/report-late-applications-protecting-students-civil-rights-in-the-digital-age/ [↑](#footnote-ref-34)
34. Christopher Libby and Jesse Ehrenfeld, “Facial Recognition Technology in 2021: Masks, Bias, and the Future of Healthcare,” *Journal of Medical Systems* (2021) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7891114/; Nicole Martinez-Martin, JD, PhD, “What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care?” *AMA Journal of Ethics: Policy Forum* (February 2019) https://journalofethics.ama-assn.org/article/what-are-important-ethical-implications-using-facial-recognition-technology-health-care/2019-02. [↑](#footnote-ref-35)
35. David Heun, “Facial recognition tech is catching on with banks,” *American Banker* (13 September 2021) https://www.americanbanker.com/news/facial-recognition-tech-is-catching-on-with-banks; Leeloo Tang, “Revisiting Facial-Recognition Payment: Old Problems Still Lingering,” *Nielsen Norman Group* (20 March 2022) https://www.nngroup.com/articles/facial-recognition-payment/; Ryan Browne, “Mastercard launches tech that lets you pay with your face or hand in stores,” *CNBC* (17 May 2022) https://www.cnbc.com/2022/05/17/mastercard-launches-tech-that-lets-you-pay-with-your-face-or-hand.html. [↑](#footnote-ref-36)
36. Jonathan Keane, “Facial Recognition Apps Are Leaving Blind People Behind,” *Vice* (22 March 2016) https://www.vice.com/en/article/ezpzzp/facial-recognition-apps-are-leaving-blind-people-behind;. [↑](#footnote-ref-37)
37. Chaz Arnett, “Race, Surveillance, Resistance,” *Ohio State Law Journal* Vol. 81 Iss. 6 (2020), pg. 1103-1142 https://heinonline.org/HOL/Page?handle=hein.journals/ohslj81&div=40&g\_sent=1&casa\_token=B-4txMbiYQEAAAAA:5h\_-tQqGl4mEH\_Lzbg1NcVrphvd8SSnKcr1qTu2hP3B4KnffJ2LwExqcT-T80ALTBDcjxtdL&collection=journals [↑](#footnote-ref-38)
38. Nicol Turner Lee and Caitlin Chin, “Police surveillance and facial recognition: Why data privacy is imperative for communities of color,” *Brookings TechTank* (12 April 2022) https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ [↑](#footnote-ref-39)
39. Arnett (2020). [↑](#footnote-ref-40)
40. Ibrahim Bechrouri, “The Informant, Islam, and Muslims in New York City,” *Surveillance & Society* Vol. 16 (2018), pg. 459-472 https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6895/8426; Rachel L. Finn, “Surveillant staring: Race and the everyday surveillance of South Asian women after 9/11,” *Surveillance & Society* Vol. 8 (2011), pg. 413-426 https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/4179/4181 [↑](#footnote-ref-41)
41. Finn (2011) [↑](#footnote-ref-42)
42. Wendy A. Bach, “The Hyperregulatory State: Women, Race, Poverty, and Support,” *Yale Journal of Law and Feminism* Vol. 25 Iss. 2 (2014), pg. 318-379 https://openyls.law.yale.edu/bitstream/handle/20.500.13051/7059/12\_25YaleJL\_Feminism317\_2013\_2014\_.pdf?sequence=2&isAllowed=y; Michele Estrin Gilman, “The Class Differential in Privacy Law,” *Brooklyn Law Review* Vol. 77 Iss. 4 (2012), pg. 1389-1445 https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1140&context=blr. [↑](#footnote-ref-43)
43. Gilman (2012) [↑](#footnote-ref-44)
44. Ibid. [↑](#footnote-ref-45)
45. Ibid. [↑](#footnote-ref-46)
46. Nicol Turner Lee and Caitlin Chin, “Police surveillance and facial recognition,” Brookings, https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ [↑](#footnote-ref-47)
47. Ibid. [↑](#footnote-ref-48)
48. Ibid. [↑](#footnote-ref-49)
49. Ibid. [↑](#footnote-ref-50)
50. Mark MacCarthy,”Mandating fairness and accuracy assessments for law enforcement facial recognition systems,” Brookings, https://www.brookings.edu/blog/techtank/2021/05/26/mandating-fairness-and-accuracy-assessments-for-law-enforcement-facial-recognition-systems/ [↑](#footnote-ref-51)
51. Ibid. [↑](#footnote-ref-52)
52. [↑](#footnote-ref-53)
53. Ibid. [↑](#footnote-ref-54)
54. ”Demographic Fairness in Biometric Systems: What do the Experts Say?” https://arxiv.org/pdf/2105.14844.pdf [↑](#footnote-ref-55)
55. Garvie (2022). [↑](#footnote-ref-56)
56. Sophia Fox-Sowell, “ACLU endorses Senate bill to ban facial recognition at airport security,” StateScoop, November 30, 2023 [https://statescoop.com/aclu-endorses-senate-bill-ban-facial-recognition-airport-security/https://statescoop.com/aclu-endorses-senate-bill-ban-facial-recognition-airport-security/](https://statescoop.com/aclu-endorses-senate-bill-ban-facial-recognition-airport-security/); Walter Wuthmann, “Mass. Bill would curb police use of facial recognition technology,” wbur, November 21, 2023 [https://www.wbur.org/news/2023/11/21/massachusetts-police-facial-recognition-ruleshttps://www.wbur.org/news/2023/11/21/massachusetts-police-facial-recognition-rules](https://www.wbur.org/news/2023/11/21/massachusetts-police-facial-recognition-rules); Christian Olaniran and Paul Gessler, “Baltimore City seeks to regulate facial recognition technology,” WJZ News, November 15, 2023 https://www.cbsnews.com/baltimore/news/baltimore-city-council-to-hold-first-public-hearing-on-facial-recognition-bill/ [↑](#footnote-ref-57)