U.S. COMMISSION ON CIVIL RIGHTS

+ + + + +

MARCH BRIEFING

+ + + + +

FRIDAY, MARCH 8, 2024

+ + + + +

The Commission convened via Video Teleconference at 10:00 a.m. EST, Rochelle Garza, Chair, presiding.

PRESENT:

ROCHELLE GARZA, Chair

VICTORIA NOURSE, Vice Chair

J. CHRISTIAN ADAMS, Commissioner

STEPHEN GILCHRIST, Commissioner

GAIL HERIOT, Commissioner

MONDAIRE JONES, Commissioner

PETER N. KIRSANOW, Commissioner

GLENN MAGPANTAY, Commissioner

MAURO MORALES, Staff Director

STAFF PRESENT:

ROBERT AMARTEY

DAVID BELL

CODY BOWER

BRIDGET BREW

SHERYL COZART

BARBARA DE LA VIEZ

PAMELA DUNSTON, Chief, ACSD

LATRICE FOSHEE

ALFREDA GREENE

DAVID GANZ, General Counsel & Parliamentarian

JULIE GRIECO

JOE KIM

TINALOUISE MARTIN, Director, OM

PILAR MCLAUGHLIN-VASQUEZ

DAVID MUSSATT, Director, RPCU

JULIAN NELSON-SAUNDERS, ASCD

PRINCE OLUBAKINDE

ESSENCE PERRY, ASCD

JOHN RATCLIFFE

ANGELICA RORISON, Director, PAU

MARK SPENCER

SYDNEY RICHARDSON-GORSKI

MARIK XAVIER-BRIER, Director, OCRE

MICHELE YORKMAN-RAMEY, ASCD

COMMISSIONER ASSISTANTS PRESENT:

NATHALIE DEMIRDJAIN-RIVEST

ALEXIS FRAGOSA

JOHN K. MASHBURN

CARISSA MULDER

THOMAS SIMUEL

IRENA VIDULOVIC

STEPHANIE WONG

YVESNER ZAMAR

A G E N D A

P-R-O-C-E-E-D-I-N-G-S

(10:01 a.m.)

CHAIR GARZA: This briefing of the United States Commission on Civil Rights comes to order at 10:01 a.m. Eastern Time on March 8, 2024, and takes place at the Commission headquarters at 1331 Pennsylvania Avenue Northwest, Suite 1150, Washington, D.C. 20425.

Good morning, everyone. I am the chair of the Commission, Rochelle Garza. And joining me today in person for this briefing are Commissioner Adams, Commissioner Gilchrist, Commissioner Heriot and Commissioner Jones.

On the phone, if you can confirm you are present after I say your name, I believe we have Vice Chair Nourse? Commissioner Kirsanow?

COMMISSIONER KIRSANOW: Here.

CHAIR GARZA: Commissioner Magpantay?

COMMISSIONER MAGPANTAY: All here.

CHAIR GARZA: Great. Will the court reporter confirm for the record that you are present?

COURT REPORTER: Present.

CHAIR GARZA: Mr. Staff Director, will you confirm that you are present?

MR. MORALES: I am present.

CHAIR GARZA: Wonderful. I welcome everyone to our briefing titled, The Civil Rights Implications of the Federal Use of Facial Recognition Technology. Our focus today centers on the civil rights implications of facial recognition technology, or FRT. We are going to be using that acronym.

It is a subject that demands our urgent attention as we navigate the complexities of today's technology's role in our society.

We aim to unpack the nuances of FRT's development, its deployment by key federal agencies, the civil rights concerns it brings to the forefront and most importantly the crucial safeguards needed to mitigate potential violations of these rights.

And while many government entities use facial recognition technology, the focus of today's briefing are on three cabinet agencies, the U.S. Department of Justice, or the DOJ, the U.S. Department of Homeland Security, DHS, and the U.S. Department of Housing and Urban Development, or HUD.

FRT is advancing at an unprecedented pace, finding its way into policing, public housing, airports and other public spheres.

And while the technology offers potential benefits, it also possesses serious threats to our

fundamental rights. It's crucial we examine these issues with the lens of civil rights at the forefront.

One of the most pressing concerns of FRT is its disproportionate impact on marginalized groups, people of color, LGBTQ individuals, women, people with disabilities, really just minorities, are often unfairly targeted by this technology. Take for instance, the cases of Robert Williams, Michael Oliver and Nijeer Parks, all Black men wrongfully identified and arrested due to flawed FRT.

These are not isolated incidents but examples of a systemic issue. And beyond the issue of bias, FRT poses a stark threat to our constitutional freedoms that has the potential to infringe on our rights to privacy, free speech and association.

Imagine a society where your every public move, habit, and association is tracked. It's a scenario that eerily mirrors dystopian fiction, yet it's becoming a reality with the advancement of this technology.

And it is for this reason and a bevy of others that the Commission had undertaken the responsibility to analyze how FRT is developed, how it is being utilized by federal agencies and find the necessary safeguards the federal government is

implementing to mitigate these potential civil rights violations.

And as we delve into these issues today, we are going to hear from a wide array of stakeholders and subject matter experts that include government officials, law enforcement, academics, researchers, industry and legal experts.

We unfortunately will not have representatives from the Department of Justice or Housing and Urban Development testifying in person today. However, we anticipate their submission of written testimony and look forward to reviewing it.

Today's public briefing marks this Commission's first step towards investigating the breadth of the challenges that FRT may pose and moving toward solutions that respect and safeguard all of our civil liberties.

We are going to hear from four panels that cover the following. The first panel will cover understanding facial recognition technology and civil rights implications. Panel 2 will cover federal government utilization and safeguard implementation of facial recognition technology. Panel 3 will cover guidance for meaningful federal oversight. Panel 4 will cover actions for strengthening responsible

federal facial recognition technology practices and policies.

And following the conclusion of the hearing, the Commission will accept written public comments until April the 8th of 2024.

So I would like to thank all of the individuals who joined us today to focus on this critical topic. Your testimony will help us fulfill our mission to be the nation's eyes and ears on civil rights.

And finally, I would like to thank the Commission staff, including our special assistants, the Office of Civil Rights Evaluation, General Counsel, our technology team that makes all of this possible, and everyone who has supported this briefing substantively and logistically.

I am now going to turn the floor over to Commissioner Mondaire Jones, the lead commissioner on this report who has spearheaded this topic.

COMMISSIONER JONES: Thank you so much, Chair for your leadership and for your vision. I want to thank my fellow commissioners for their support of today's hearing.

On the first topic that I proposed as a new member of this body, I am especially proud of

having worked in a bipartisan fashion, which is rare these days, with my colleague, Commissioner Gilchrist, to get my proposal across the finish line.

It is as much a testament to our ability to actually function even as we are oftentimes evenly divided as it is a testament to the universal concern that Americans have about the issue of facial recognition technology in particular and, of course, artificial intelligence more generally.

I want to thank the Commission staff, especially my special assistant, Irena Vidulovic, for their hard work in the months and the days leading up to today's briefing.

Today's hearing, and our subsequent report, as you have heard, will analyze how facial recognition technology is developed, how it is being used by the federal government, emerging civil rights concerns and safeguards that the federal government can and should implement to address what we are clearly seeing as glaring civil rights issues.

In particular, this project will review the use of facial recognition technology by the Department of Justice, Homeland Security and Housing and Urban and Development.

I want to thank DHS in particular for

participating in today's briefing, both through its written testimony and through the numerous representatives that it has sent to testify today in person. I appreciate that DHS takes its statutory obligations and the work of this Commission seriously.

By contrast, I find it not just disappointing but offensive that DOJ and HUD declined our invitation to appear in person today and thus far have not even submitted written testimony. I have not seen anything like this from this administration and have the Commission been given adequate notice of the failure of these Departments to cooperate, I would have urged this Commission to exercise its statutory authority to issue subpoenas, which is something that we have rarely had to do in the course of this Commission's existence.

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.

I also believe that their approach is a

strategic error because now Congress is going to pay even closer attention and so will the press, which is well represented here today, and most importantly so will the American people.

Along with representatives from DHS, I am delighted that our briefing will have in-person testimony from subject matter experts, academics, researchers, software developers, civil rights and civil liberties advocates, the White House, and of course, legal experts.

The Commission has also received written testimony from my former colleagues, Congresswoman Yvette Clark and Congressman Ted Lieu, who lead important legislation in the House that deals with FRT broadly, and is used by HUD specifically.

Over the past few years, facial recognition technology has come under the scrutiny of civil rights advocates, legislative bodies and the public as the use this technology continues to grow.

The use of FRT has become increasingly common across the federal government. In fact, a report by the Government Accountability Office, or GAO, show that 18 of 24 surveyed federal agencies use FRT for one or more purposes.

Another study of 42 agencies that employ

law enforcement officers found that 14 of those agencies use FRT. Of those, 13, "did not track employee use of nonfederal, for example state and commercial FRT systems.

GAO found that employees were not aware that they were using nonfederal FRT systems and yet had conducted more than 1,000 facial recognition searches."

Since there was widespread use of FRT in the federal government, the Commission has embarked on this important task to ensure that the federal government is protecting civil rights by making sure that processes and protections exist, transparency is applied and accountability is enforced.

So I look forward to listening and learning today from experts who have for years been on the front lines of using, studying, and safeguarding against this technology. Thank you so much again.

CHAIR GARZA: Yes, Commissioner?

COMMISSIONER ADAMS: Can I just be recognized for just a brief comment?

CHAIR GARZA: Sure. That's fine.

COMMISSIONER ADAMS: 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 pow er.

But I want to see your problem and raise you one. The Office of Legal Counsel at DOJ, OLC and the Civil Rights Division, CRT, are going to be the primary drivers of any federal policy related to facial recognition technology.

DHS has their own Civil Rights Office that it's effectively subservient to whatever OLC or CRT says about the policy. So not having them here takes away the central organizing component of the federal government to answer these questions.

So I support you and your concern and whatever steps you think are appropriate going forward.

CHAIR GARZA: Thank you, Commissioner Adams and thank you Commissioner Jones for your statement.

I am now going to turn this to our briefing with a few housekeeping items. During the course of the testimony and the question and answer period, I caution all speakers, including Commissioners, to refrain from speaking over each

other for ease of transcription and to allow for sign language translation.

I would ask that we allow any individuals who might need to view the sign language translation to sit in the seats with a clear view.

For any member of the public who would like to submit materials for our review, as I mentioned, we are going to be accepting materials through April the 8th of 2024. You can submit your materials by mail to the U.S. Commission on Civil Rights, Office of Civil Rights Evaluation a 1331 Pennsylvania Avenue Northwest, Suite 1150, Washington, D.C. 20425, or by email. And the email address is frt@usccr.gov.

During the briefing, each panelist will have seven minutes to speak. After each panel presentation, Commissioners will have the opportunity to ask questions within the allotted period of time, and I will recognize any Commissioner who wishes to speak.

I will strictly enforce the time allotments given to each panelist to present his or her statement. And unless we did not receive your testimony until today, you may assume that we've read it. So you can summarize it, and we will appreciate

that so that you can make the best use of your time under seven minutes.

I ask my fellow Commissioners to be cognizant of the interest of each Commissioner to ask questions. So please be brief in asking your question so that we can move quickly and efficiently through today's schedule. I will step in to move things along if needed, although I don't anticipate that.

Panelist, please notice the system of warnings lights that are in front of you. When the light turns from green to yellow, that means two minutes remain. When the light turns red, panelists should conclude your statements so you don't risk me cutting you off. My fellow Commissioners and I will do our part to keep our questions and comments concise.

And now we're going to turn to our first panel, Understanding Facial Recognition Technology and the Civil Rights Implications. And I am going to go ahead and introduce our speakers. Thank you all for being here.

And the order you will be speaking is Bertram Lee, and I apologize if I mispronounce your name, Technology Policy Expert, Gretta Goodwin, PhD, Director, Homeland Security and Justice, U.S.

Government Accountability Office, Hoan Ton-That, founder and CEO of Clearview AI, Armando Aguilar, Assistant Chief, City of Miami Police Department. Michelle Ewert, Professor and Director of a Law Clinic at Washburn University School of Law, and Katie Kinsey, Chief of Staff, Policing Project, New York, NYU School of Law.

(Panelists sworn.)

CHAIR GARZA: Affirmative from all. Mr. Lee, could you please begin?

PANEL 1: UNDERSTANDING FRT AND CIVIL RIGHTS IMPLICATIONS

MR. LEE: Thank you, Chair Garza, Vice Chair Nourse and distinguished members of the Commission. My name is Bertram Lee, and I am here in my personal capacity. The views that I express during today's hearing do not represent those of the National Telecommunications and Information Administration or of the Department of Commerce.

Thank you for the opportunity to testify about the use of facial recognition technology by federal agencies.

The last time I testified on this topic almost 30 years ago in front of the House Judiciary Subcommittee on Crime, Terrorism and Homeland

Security, the AI revolution was just beginning, if you could have foreseen the broad adoption and impact that artificial intelligence would have on government and our society at large.

While the AI landscape has changed, unfortunately, the many issues concerning facial recognition have not. I want to leave the Commission with three main points that are still unfortunately germane to the conversation around federal use of facial recognition technology today.

One, facial recognition technologies are inherently biased. Two, improving accuracy will not mitigate the disparate impact of facial recognition technology. And three, facial recognition technology only expand the current police state in frightening ways.

Facial recognition technologies are inherently biased. And facial recognition technology still disproportionately misidentify and misclassify people of color, trans people, women and other marginalized groups posing threats to community's health, safety and well-being.

The reasons for these biases vary. In some case the cause of the bias is the database and images being shared against, and in others it is due

to historical bias that is built into these systems and who trained it.

While the technology has improved due to technical advancements and use of neural networks, the reality is that broad discrepancies remain between the different demographic groups based on age and race.

For example, Clearview AI's facial recognition system was shown by the National Institute of Science and Technology in a December study to be more than 400 times more likely to misidentify Black women over 65 than young white men ages 20 to 35.

While demographic testing is still ongoing through the NIST process, foundational discrepancies and the accuracy of facial recognition technology are still very much relevant today. There has been a long struggle for darker skinned people to have their images accurately captured on camera.

This fundamental flaw is now baked into databases and AI systems that are continuing to entrench discriminatory outcomes. There are now at least seven people that we know of that have been misidentified by facial recognition technologies. These interactions with law enforcement can have life altering impacts on the lives of those people. Improving accuracy will not mitigate the disparate

impact of facial recognition.

Improving the accuracy of facial recognition technology will not address the fundamental issue that facial recognition technology expands of scope of power of law enforcement and federal agencies.

As the recent letter from 18 U.S. senators highlighted, there are not only legal implications for government use of these technologies but also First Amendment, civil rights and civil liberties implications as well.

From the use of facial recognition technology to track Black Lives protestors to my previous back and forth with House Judiciary Chairman Jim Jordan, there are bipartisan concerns about the use of facial recognition technology by the government.

Third, facial recognition technologies will only expand the current police state. Facial recognition technologies have expanded the current police state and also the commercial surveying state. Sadly, when I testified previously the lack of oversight on facial recognition was staggering. Three years later, the situation is even more dire than we could have imagined.

In 2016, a Georgetown group that included current FTC Commissioner Alvaro Bedoya highlighted that more than 119 million U.S. adults were in some sort of facial recognition database. That number grew in 2019. And now a majority of Departments of Motor Vehicles in the U.S. use some form of facial recognition technology. These systems are connected to broader federal and local law enforcement databases with very little training.

A 2023 GAO study on federal law enforcement agencies' use of facial recognition technology highlighted the fact that only two of the seven law enforcement agencies require any training on the technology as of April 2023.

Due to the number of searches in different facial recognition systems used, the broad access to these technologies and full accountability is almost impossible.

In conclusion, evidence that facial recognition technology impedes civil and human rights has never been clearer. Facial recognition technology and the biases that these systems contain only serve to continue this history of discrimination and disparate treatment of people of color.

In the past three years, the continued

expansion of surveillance technologies like facial recognition have not made communities of color safer. Instead, it has done the opposite. The use of facial recognition only by federal agencies only further exposes people of color to systemic racism of the criminal legal system, reinforcing racist scenarios that Black communities and other people of color are to be surveilled and over policed at every turn.

I urge the Commission to further investigate the use of facial recognition technology by the federal government and to do what it can to shed light of the severe consequences that continued use of these technologies can have on the most vulnerable communities.

I thank the Commission for the opportunity to address the serious concern of this technology, and I look forward to answering your questions.

CHAIR GARZA: Thank you, Mr. Lee. We will now hear from Dr. Goodwin.

DR. GOODWIN: Chair Garza, Vice Chair Nourse and members of the Commission. Thank you for the opportunity to discuss GAO's work on the use of facial recognition technology by federal and law enforcement agencies.

The capabilities and uses of this

technology has expanded in recent years and questions exist regarding the accuracy of the technology, the transparency in its usage and the protection of privacy and civil rights.

Facial recognition technology is a powerful tool that federal law enforcement agencies may use to help solve crimes. The technology allows law enforcement to quickly search through billions of photos to help identify an unknown suspect or victim in a crime scene photo or video.

While the technology may support criminal investigations and help bring bad actors to justice, policymakers and federal agencies must consider the potential impact of its use on civil rights and civil liberties because the potential for error and the potential to misidentify someone could lead to the arrest and prosecution of an innocent person.

Civil liberties advocates have also noticed that the use of facial recognition at certain events like protests could have a chilling effect on an individual's exercise of their First Amendment Rights.

GAO issued reports in 2021 and 2023 related to federal law enforcement's use of the technology. Today I will focus on the information we

learned from seven law enforcement agencies within DOJ and DHS, the FBI, the DEA, the ATF, U.S. Marshals, Customs and Border Protection, Homeland Security Investigations and the Secret Service.

I will discuss the extent to which these law enforcement agencies owned and used the technology, developed policies to help protect civil rights and civil liberties, required staff to take training and have taken steps to address selected privacy requirements.

In 2021, we reported the results of a survey that we sent to law enforcement to federal agencies that employ law enforcement officers regarding their use of the technology.

Federal agencies used this technology to support various law enforcement activities. For example, it was used by the ATF in an arson investigation. The individual was ultimately arrested, confessed to the arson and was sentenced.

We also learned that the technology was used to support criminal investigations related to the civil unrest following the killing of Mr. George Floyd in May of 2020. The agencies reported that these searches were on images of individuals suspected of violating the law.

After the Capitol attack of January 6, 2021, the technology was used to generate leads and support criminal investigations. Last year, we analyzed the use of facial recognition services by commercial and nonprofit entities.

The law enforcement agencies reported using four services in total from October 2019 to March 2022. All seven law enforcement agencies initially used these services without requiring their staff to take training on topics such as how the technology works, what photos are appropriate to use, and how to incorporate the results. About 60,000 searches were conducted before staff were required to take this type of thing.

We also reported that three agencies had policies specific to protecting civil rights and civil liberties when using the technology. While the remaining agencies did not have guidance or policies in place, officials told us that staff must abide by more general guidance that helps ensure these protections during investigations.

I want to note that DHS has since issued a policy which includes topics such as limiting the use of the technology, protecting privacy, civil rights and civil liberties, and testing and evaluating the

technology.

DOJ officials told us they plan to issue a department-wide policy on facial recognition technology. Until that policy is finalized, they have issued interim guidance to help safeguard civil rights and civil liberties.

We also reviewed DHS and DOJ's privacy requirements around the use of facial recognition services. We found mixed results. Three of the agencies addressed some of the privacy requirements. The remaining four did not fully address any of the requirements.

Program officials told us that they didn't fully address the requirements in part because they didn't initially recognize photos as personally identifiable information. They didn't realize staff had transmitted photos to facial recognition services or they didn't fully coordinate with their privacy officials while acquiring these services.

We made recommendations to DOJ and DHS related to privacy requirements. Both concurred with our recommendations. As of February 2024, they had not implemented our recs.

As the capability and usage of facial recognition technology and other biometric

technologies increase, it is important that the appropriate private and civil liberties protections are in place.

While these services may support investigations, our work has shown that additional federal actions are needed to help prevent potential abuses and to increase the public's confidence in law enforcement's use of this technology.

Chair Garza, Vice Chair Nourse and members of the Commission, this concludes my remarks. I'm happy to answer any questions you have.

CHAIR GARZA: Thank you so much, Dr. Goodwin. We're going to now hear from Mr. Ton-That. Please proceed.

MR. TON-THAT: Dear Commissioner Garza and everyone else on the Commission. It's an honor and a pleasure to participate in our conversation today, which covers a very important topic of this technology's impact on civil rights.

As a person of mixed race, it is especially important to me that this technology is supporting the world in a way that protects and enhances civil rights.

I am Hoan Ton-That. I am the founder and CEO of Clearview AI, a facial recognition search

engine company. 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.

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.

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 accidentally for just a second. They had no other

clues or ways to identify the perpetrator so they turned to Clearview AI.

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.

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.

They found thousands of 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.

This is a great example of how facial recognition is used in practice. First it shows that investigative work is required to verify an identity after getting a result from facial recognition and that human investigators are making the final judgment.

Secondly, it shows the true impact of facial recognition and how it can combat the most heinous of crimes. The director of Homeland Security in that unit at the time said without Clearview AI, there is no way that they would have found that guy.

The second example is actually regarding a public defender's usage of facial recognition technology to exonerate someone wrongfully accused of a crime he did not commit.

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.

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. 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 were able to get 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.

This was a long ordeal for Andrew, but it also shows the flip side of facial recognition and how it can be used by public defenders to protect the innocent.

While some may point to demographic differentials for facial recognition algorithms, what truly really matters is absolute accuracy. Clearly these algorithms can testify NIST FRVT program, which measures accuracies using large data sets and millions of diverse photos of varying quality and poses. The algorithm is shown to be 99 percent accurate across every demographic group and test category.

In fact the one to N FRDT test, which is the hardest one to do, the algorithm can pick the correct fact out of a lineup of 12 million photos at

an accuracy rate of 99.85 percent. That's much better than a human eye. Can you think of anyone who could find the correct photo out of 12 million and that level of accuracy consistently?

I really do believe that accurate facial recognition with the appropriate controls, regulation and training will decrease bias in policing.

First, when law enforcement currently encounters a photo of a suspect for camera footage and is unable to identify them, they put out a bolo, a be on the lookout for an alert, to law enforcement agencies with a description of the suspect, which typically includes race, gender and physical description.

This causes law enforcement to look for suspects who match that description and question many people who are innocent who are not the suspect. It also involved things like unnecessary traffic stops and other police interactions with those who are innocent in the community.

And so facial recognition, I truly believe once accurate can decrease unneeded police interactions and, you know, further trust with the community and the police.

Secondly, police should have access to a

facial recognition system that services the broad population, not just photos of people who have been arrested before. Clearview AI's database has not just mugshots. It contains people from public internet. This helps prevent bias against communities of color and the narrow population of people who have arrest records.

You can find more about this in my written statement and thank you for your time.

CHAIR GARZA: Thank you so much for your testimony. Now we are going to proceed with Chief Aguilar.

MR. AGUILAR: Good morning, Chair Garza, Vice Chair and members of the Commission. I am Armando Aguilar, Assistant Chief of Police with the Miami Police Department. I am also currently serving in a three year term as a member of the Law Enforcement Subcommittee of the National Artificial Intelligence Advisory Committee, or NIACLE. I would, however, like to point out that I am speaking today on behalf of the Miami Police Department and not on behalf of NIACLE.

I am proud to say that the Miami Police Department story is among the greatest turnaround stories in law enforcement. In 1980, Miami, with a

murder rate comparable to that of Honduras, was America's murder capital.

I became a Miami police officer in 2001 and a homicide detective in late 2004, a year where 69 people would be murdered in Miami and another 6,400 would fall victim to violent crime.

By this time, we had the audacity to high five each because at least we were no longer in the top five most violent cities in America. We were, though, perennially listed among America's top 25 most violent cities per capita.

Fast forward to last year, to 2023, Miami ended the year with 31 murders and 2,600 violent crimes. Still 31 and 2,600 too many but a move in the right direction.

Our murder clearance rate, the rate at which cases were solved last year was 71 percent or 97 percent if we use the FBI's legacy reporting system which credits solved cold cases. Our violent crime clearance rate was 58 percent.

Now for perspective, for most of my career, that murder clearance rate hovered around 45 percent and our violent crime clearance rate below 38 percent. So what changed? Well, a great deal. I will begin by stating that I have had the pleasure of

leading the best generation of officers, detectives, and professional staff to ever serve the people of Miami.

It all begins with community trust. Violent crime, especially unsolved violent crime, is among the greatest threats that serves 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 gun fire 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.

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.

We use ballistic evidence to connect the dots between shooting and violent actors victimizing our communities. A recent BJA funded study by Florida International University found that crimes where one such resource was used by our detectives had a 66 percent great likelihood of being solved when compared against similar cases where no such resource was used.

I am happy to discuss any of the technologies that we employ, but I will take this remaining time to discuss how we came to develop our policy governing the use of FRT in criminal investigations.

For us it started in 2020 when the New York Times ran an article that was critical of law enforcement use of FRT and of one company in particular.

The author of the article, Kashmir Hill, posed several questions that resonated with me as I do spend my time out of uniform as a private citizen. Without proper safeguards, Mr. Hill asked, what would stop police from using FRT to identify peaceful protest organizers or stalking an attractive stranger at a café? And what about the public whose biometric data, i.e., our faces, would be used by police? What

sort of public input should be sought when deploying such technologies?

My team and I set out to establish a FRT policy that would address these and other concerns. We were not the first law enforcement agency to use facial recognition or develop FRT policy, but we were the first to be this transparent about it. We did not seek to impose our police on the public. We asked them to help us write it.

We started out by meeting with local privacy advocates, and they absolutely hated it. But we wanted to know why they hated it. So they were very happy to tell us. We found many of their critiques to be thoughtful and reasonable. So we heard their objections, took it upon ourselves to treat them as recommendations, and we incorporated several of them into our policy.

We highlighted successful arrests, aided by FRT for local media coverage. That March we held two virtual town hall style meetings. In-person meetings were not an option due to the pandemic.

We conducted one session in English. One session in Spanish. Each session, which included public questions and comments, had about 1,300 live views and 3,600 total views.

The policy that resulted from our efforts created a narrow framework within which we would come to use FRT. Most importantly, our policy emphasizes that face recognition matches do not constitute probable cause to arrest. Matches are treated as anonymous tips, which must be corroborated by physical testimony or circumstantial evidence.

We laid out five allowable uses, criminal investigations, Internal Affairs investigations, identifying cognitively impaired persons, deceased persons and lawfully detained persons.

We use it retrospectively. That is we are not using it on a live or real-time basis to identify people going about their business in public spaces or use it to identify people who are carrying out constitutionally protected activities such as free speech or religion.

We establish a policy limiting who has access to our platforms, and we disclose our use of facial recognition to defense counsel in criminal cases. We do not substantively manipulate or alter probe photographs, use composite sketches as probe photographs or use any other technique that has not been scientifically validated.

These efforts, along with many others,

have resulted in a Miami that is safer today than in any other time in our history. I thank you for inviting me to testify before the Commission today. And I am happy to answer any questions that you may have. Thank you.

CHAIR GARZA: Thank you, Chief Aguilar. We are going to now hear from Professor Ewert. Please proceed.

MS. EWERT: Good morning and thank you to the Commissioners for considering this important issue and for inviting me to speak with you today.

I am going to talk to you about how FRT is currently being used in affordable housing in general and subsidized housing, like public housing in particular, and the particular ways that it harms tenants.

So I will talk first about current uses and then about the problems that stem from those uses.

So how is FRT being used today? First for building access. More apartment complexes are using facial scans instead of keys or fobs to unlock doors into apartment buildings and within apartment buildings. And the rationale is that a tenant could lose their key or lose their fob and that FRT is safer, but I will talk to you about some of the

problems that tenants in these buildings are having.

The second use is tenant surveillance. We're seeing cameras outside and inside buildings surveilling tenants, monitoring them, livestreaming those feeds to Police Departments or else sharing those recordings with law enforcement after the fact, so essentially warrantless searches and warrantless surveillance. And the rationale here is that this is supposed to deter crime and help police identify perpetrators.

The 2023 Washington Post article that I included with my supplemental materials talks about the increased use of surveillance cameras in public housing. For example, the number of cameras per tenant in the Rolette, North Dakota, public housing program rivals that of the number of cameras per inmate at Rikers Island.

There are increasing concerns that use of this technology is not just for building access and tenant surveillance, that those are sort of pretextual in some situations, and that rather landlords are using these to evict tenants to get rid of low income residents and then convert subsidized or affordable units to market rate units.

And the Law Journal article that I

submitted with my supplemental materials actually includes examples of how tech companies are advertising this as a way to get rid of affordable housing.

So why is this use of FRT problematic for subsidized tenants? First, the technology is flawed. You heard Bertram Lee testify about inaccuracies based on race and gender and age, so I am not going to belabor that point. But I will say that these problems or these inaccuracies are especially problematic for subsidized housing tenants who are disproportionately women, disproportionately people of color and disproportionately seniors.

Conditioning access to one's home on technology that does not consistently recognize you or household members just doesn't make sense. And this is the complaint of tenants at Knickerbocker Village, a complex in New York that has been using FRT for building access for a little over 10 years.

The tenants in this apartment complex are mostly of Chinese descent and they complain about the technology not recognizing them consistently, having to stand outside in the rain and the cold because they can't get in. Having to wait for a neighbor to exit to let them in or a security guard to come by. So

people are being denied access to their housing if the technology doesn't recognize them.

But even if the technology could be improved in the future to recognize people better across, you know, gender and age and race, more serious privacy concerns would still persist. And that is what I want to focus the rest of my time on, how the use of FRT and surveillance invades the privacy of people who have no real alternative but to submit to this surveillance and screening.

And these privacy concerns were raised by the residents in Atlantic Plaza Towers, an apartment complex also in New York, over 700 units, mostly Black female tenants.

And the privacy concerns that they raised in their complaint to the State Office of Rent Administration when their landlord proposed to implement this technology, and what advocates and tenants around the country have identified, those privacy concerns are threefold.

First, use of FRT in surveillance in this context conditions people's entry into their home on surrendering biological data to third parties. So the landlord contracts with the AI company, who administers a technology and then stores that

biometric data. But we are all, you know, reading week after week about the increase in cyber attacks so this use for subsidized tenants increases the odds of their biometric data being released in one of these data security breaches.

The second privacy concern that tenants have identified is that this creates a record of their movements and their associations in and around the apartment complex. Some low income tenants of color describe this as being like having an ankle monitor, but I argue this is actually more invasive than that because it not just tracks location, it also sends images of people who are not accused of any crime, not convicted of any crime.

Landlords know when people arrive in the building, when they leave, with whom the tenants speak, where they go, and this could have a chilling effect on participation in things like tenant association meetings, things like that.

And this is one of the issues that the tenants at Atlantic Plaza Towers raised in their complaint. The landlord was pulling out screenshots of the tenants and sending it to them, basically trying to intimidate them to stop their tenant organizing.

The third privacy issue that comes up in this context is the interference with personal relationships because the system surveils not just the tenants themselves but also their guests and their family members. And it can incentivize people not to come and visit if they are afraid that one, they might be misidentified as someone who has a warrant out for them if there is a false positive or if they don't want to risk their, you know, biometric data being released in a cyberattack.

So it makes it harder for vulnerable tenants like seniors or people with disabilities to get help from their social networks, especially if the surveillance is being done in conjunction with law enforcement.

So to wrap up, low income tenants have few options for affordable housing. If they forego rent controlled units or subsidized housing, they are stuck on the private rental market where they face the risk of eviction if they can't consistently pay rent. So the use of FRT and surveillance in this context forces people to give up their biometric data and their privacy just to have safe, affordable housing.

I am happy to answer questions afterwards. But thank you for your time.

CHAIR GARZA: Thank you so much professor. We are going to now hear from our last presenter on our first panel, Ms. Kinsey, you can proceed.

MS. KINSEY: Thank you to the Commission and the staff for calling this important public briefing on law enforcement use of facial recognition technology, our federal use. My remarks will focus on the law enforcement context.

My organization, the Policing Project, at New York University School of Law works to promote public safety through transparency, equity, and democratic accountability.

By democratic accountability, we mean that there needs to be democratically approved rules, laws and policies in place before policing agencies act. Policing, especially when it comes to the use of emerging technologies and facial recognition, suffers from a lack of this kind of front-end accountability today. This is both undemocratic and it has caused harm to American civil rights.

At the Policing Project, we pursue our mission of democratic accountability with all stakeholders. We work with impacted communities, civil rights and civil liberties advocates, tech companies and law enforcement themselves.

We have been researching and studying law enforcement use of facial recognition for a number of years now. And from that research, I have two main takeaways for the Commission today.

The first is that law enforcement use of this technology is non-transparent and unregulated and this is causing harm to American civil rights.

The second is that if law enforcement is going to continue to use this technology, it has to be regulated. That is the bottom line. At the Policing Project, we start our evaluation of any policing technology with the same basic question. Will the public benefit from use of this tool?

Because as any good economist will tell you, when it comes to cost benefit analysis, you don't even need to evaluate cost until you have established measurable benefits.

The problem with federal law enforcement use of facial recognition today is that we lack adequate proof of public safety benefit.

Now how can I say this when you have already heard stories today about facial recognition technology being used to solve serious crime or even exonerate the wrongly accused?

What I mean is, all the public has today

are sporadic anecdotes of success or cherry-picked data often from the technology companies themselves who makes these products. And I can just as readily point to anecdotes of real harm when it's used by law enforcement. That includes false arrest. Most recently a Black woman in Detroit was falsely arrest while she was eight months pregnant, causing her to go into early labor from the use of facial recognition misidentification.

So right now we have no idea of the successful anecdotes of law enforcement use represent the tip of an iceberg or are exceptions to otherwise harmful uses.

And OMB has made clear that federal agencies should not be allowed to use technologies like facial recognition if they cannot prove measurable benefits that meaningfully outweigh the risks of use.

The problem is that we need this measurable representative data about public safety benefit of law enforcement use of this technology, and we don't have it today.

We don't have it because so far law enforcement use has been very not transparent. And what I mean by that, is we don't have answers to basic

questions about federal agency use of facial recognition technology. Questions like how often are federal law enforcement agencies running facial recognition searches, on what types of crimes, on what demographics, and to what result? Are these searches actually leading to more crimes being solved?

These are essential questions that we need the answers to if we want to make good policy but we don't have them right now. Consider the FBI as just one example. They have been running facial recognition technology since 2011. They have their own database that has over 40 million photos of American citizens in it. They have conducted 200,000 searches of this database. We don't know for what crimes. And they spent tens of millions of taxpayer dollars on this facial recognition technology.

Now the Government Accountability Office has also taught us some things about the FBI use so far and that the FBI has only limited information on the accuracy of its facial recognition system. It has no policy in place to protect from the civil rights and civil liberties implications of use. Only 5 percent of staff who have access to the system have received any sort of training. And they have no mechanism to track FBI employees' use of external

facial recognition systems.

So despite the FBI's rampant use of this technology, we have very little information about its use, and we lack meaningful oversight over this use.

Now not only is the public in the dark about how federal agencies are using this technology, we also don't know how well or poorly it works. And that's because it hasn't been tested under real world conditions.

What I mean by that is, you might have heard folks today already talk about testing conducted by the National Institute of Standards and Technology. This testing is extremely valuable, but it's also extremely limited. NIST only tests algorithms. It doesn't test complete facial recognition systems under real world conditions on things like the photos that law enforcement is actually searching or the human operators who are actually conducting the review.

So to understand the difference between NIST testing and what real world testing would look like, think about another human machine system, a Formula 1 race car. NIST testing is the equivalent of testing just a Formula 1 car's engine in isolation.

Engine testing is absolutely necessary, but it's not sufficient. If you own one of these

expensive machines, you are going to test that engine in the car, with a driver on an actual racetrack. In other words, you are going to test it in real world conditions. That's the only way you are going to know how it performs.

We don't have that kind of testing when it comes to facial recognition technology. And that means we don't know how well or poorly it works in the real world. So without knowing how law enforcement agencies are using this technology without knowing to what effect and without knowing how accurate it is, we have no way to assess the measurable public safety benefits of use. But we do know it is causing real harm. So that's the false arrest that I talked about earlier. Others, we will go into those in much more depth later. But I also want to point out that it causes another type of harm, which is it erodes community trust in law enforcement, which Chief Aguilar already noted is essential to public safety.

So this status quo is untenable. What we need instead is sound governance over law enforcement use of facial recognition. Luckily, we already have really good models for what sound governance requires here. At the Policing Project we have developed our own federal legislative checklist. OMB's guidance

recently issued in AI used by federal agencies has absolutely essential safeguards that apply to facial recognition.

The National Academies has a great recent report of governance. Representative Ted Lieu's bill provides a comprehensive framework for law enforcement use. And they all say many of the same things. We need federal regulation. We need meaningful transparency over use. We need real world testing. And we need national standards and best practices rather than the Wild West that we have out there right now.

At the Policing Project, we believe there is real promise for public safety technologies to promote public safety. A decision to use any policing technology must be democratically accountable, and they must show measurable proof of benefit. They also require a real commitment to protecting civil liberties, civil rights and racial justice. Protecting public safety and protecting civil liberties are not mutually exclusive aims.

Law enforcement agencies need to recognize this and federal law enforcement needs to -- federal policymakers need to make sure that they do. Thank you.

CHAIR GARZA: Thank you so much, Ms. Kinsey. At this point, I'm going to open it up to questions from Commissioners. So please let me know if you would like to be recognized.

Okay. Commissioner Jones, go ahead.

COMMISSIONER JONES: Thank you, Madam Chair. I have a question for Dr. Goodwin. In your written testimony, you note something that is alarming to me, which is that at least prior to December 2023, DOJ had no policy on the use of facial recognition technology that at least was intended to implement safeguards for civil rights and civil liberties.

But then in December of 2023, just a few months ago, possibly as a result of your inquiries, they implemented an interim policy, but you had not yet had an opportunity to obtain and review the policy and thus could not confirm the information that they represented. Is that because they didn't produce that policy to you? Clearly, that's not a public policy for us to review.

DR. GOODWIN: So thank you for that question, Commissioner Jones. So whenever GAO issues a report and we have recommendations, we do a recommendation follow-up. And as I mentioned, DOJ concurred with all of our recs. And when we were

doing the follow-up, that's when we were told that they have this interim policy.

We have asked for that policy. We haven't seen it. We will continue to follow-up because with the recs, we have to report back and forth to the Congress on where each agency that we've made recommendations to where they are in terms of addressing our recs. So it is something that we will continue to follow-up on.

COMMISSIONER JONES: Is it normal for an agency to represent to you that they have a policy that they are unwilling to produce to you for your review?

DR. GOODWIN: I wouldn't say -- I wouldn't use the term normal. But there is always a back and forth. When we reach out to follow-up on where the recs are, we will continue to ask for that policy. And we will continue to report back to the Congress as to whether or not we actually have it, receive anything.

And then at some point I would imagine the Congress will be asking DOJ to take a look at the policy.

COMMISSIONER JONES: Yes.

DR. GOODWIN: But again, we do rec follow-

up, and that is just part of our rec follow-up. The minute we have the policy, we will look at the policy. Do our own analysis to see if it actually meets the spirit of our recommendation.

COMMISSIONER JONES: Is DOJ under a statutory obligation to produce that document to you or does that have to be requested by some other agency?

DR. GOODWIN: Well, they have a statutory responsibility to respond to our recommendations. And so that's just part of the follow-up that we do with them. And whenever we get any information for any agency that we've made a recommendation to, we will note that information on our website, our public facing website.

So for any report that GAO ever, you know, puts out, and we have recommendations, you can go to the GAO website and go to that report. And there is a tab that says recommendations. And every single rec, and every single piece of information in terms of follow-up, whether the rec is closed, whether it's open, whether it's partially addressed, we will have all that information there.

COMMISSIONER JONES: So I'm going to let other folks ask questions. But I just -- I want to be

clear that you are unable to do your job completely in terms of ensuring compliance because DOJ has not produced this interim policy to you.

DR. GOODWIN: They have not yet produced the interim policy to us, that is correct.

COMMISSIONER GILCHRIST: Madam Chair?

CHAIR GARZA: Go ahead.

COMMISSIONER GILCHRIST: Someone else?

CHAIR GARZA: Commissioner Heriot just asked.

COMMISSIONER GILCHRIST: Okay, please.

CHAIR GARZA: Then we'll go to you.

CHAIR HERIOT: My question is for Mr. Ton-That. You know, one of the striking things about this technology is while it is imperfect, human identification is even more imperfect, many more errors. You gave the example of how sometimes this technology has worked to the advantage of the defense in a criminal case. But it was kind of an odd situation. It's a witness.

Is this technology capable of finding that a human ID is simply error? So a human being testifies the defendant did it. Has this technology ever been used to say the witness is wrong? Our machine says it's not the same person.

MR. TON-THAT: Thanks, Commissioner, for the question. Currently, the status quo for law enforcement is when they can't identify someone before and then just BOLOs, be on the lookout, getting tips and also another big issue with law enforcement today is eyewitness testimony.

So I believe the Innocence Project said that 70 percent of wrongful convictions that were later overturned because of DNA evidence came from eyewitness testimony, which is admissible in court.

The way our technology works is it just generate leads. We don't allow our facial recognition match score to be even shown to the end user.

So in the case you are thinking of, that is, I'm sure, when law enforcement is able to use accurate facial recognition like Clearview and then get other evidence, for example, say business surveillance footage of someone robbing a store, instead of relying on the eyewitnesses to say that's the person, they can be able to say run the facial recognition search, find another piece of evidence, maybe a matching tattoo or matching clothing, and use that as much more objective evidence than eyewitness testimony.

So I truly believe that accurate facial

recognition technology can really decrease reliance on eyewitness testimony, which has shown to be unreliable.

At the end of the day for defendants and for prosecutors, everyone wants to get to the truth of, you know, evidence. So this allows a more objective way of doing so. Thank you.

CHAIR GARZA: I'm going to jump in here and just ask a follow-up question to that. Aren't individuals also looking at this data? So it could complicate this problem that you're saying is solved by eyewitness testimony?

I mean, we hear from police agencies that they are also reviewing the information and looking at the matches. I mean, you know, how do you explain that if we've got a lot of people actually looking at this data?

MR. TON-THAT: Yeah. So I'm 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.

The way we've designed our technology is we give training to every user before they use the technology. We make sure the agency has been approved to run a trial of Clearview AI. The recommended

agencies have a public facial recognition policy as well.

And as part of the training, we show that this is just lead information. So I think for investigators, the more information that confirms who someone is, that disconfirms who someone is can be very valuable.

So, yes, these investigators, the more data is more likely to actually confirm the person or they think it is actually someone else. So in the example of what the status quo is today, is basically we can identify someone who is in a BOLO, be on the lookout, this has the person's like race, their gender, rough age, description, if they have tattoos or not. And that means that law enforcement isn't like pulling over people that are innocent to try and ask questions.

With accurate facial recognition, you can skip all of that stuff if you, you know, vet it properly and get the right identification. So I do believe that it does improve civil rights and civil liberties overall.

CHAIR GARZA: Is the training that we have, and then we'll go to you. I'm so sorry.

COMMISSIONER GILCHRIST: No, you're fine.

You are asking the same questions I want to ask.

CHAIR GARZA: Is it mandatory? Was that your question?

COMMISSIONER GILCHRIST: Well, no, I'm sorry, Madam Chair.

CHAIR GARZA: I'll ask my question. So is the training mandatory and is it uniform across all police agencies that you work with?

MR. TON-THAT: Yes.

CHAIR GARZA: What does it look like?

MR. TON-THAT: Since early 2020, we have a mandatory training for all users. So first we train an administrator.

So everyone who uses Clearview has a designated administrator who can oversee all the searches for that agency. So that allows the administrator to make sure they are using for a proper purpose related to law enforcement.

Then we train each of the end users, and as a requirement of Clearview before we conduct any search of the platform, we have to put in a case number and a crime type, essentially a reason for doing the search.

And so, yeah, that's what we do. That is separate from, say some of these federal agencies who

also have their own training programs. Even if an agency has its own training program, we still provide ours as well.

CHAIR GARZA: And the end user would be the police agency using.

MR. TON-THAT: Correct. So from the administrators down and the end users who are doing the investigating.

CHAIR GARZA: And the administrator would be someone in the agency as well. I will let you ask your question, Commissioner.

COMMISSIONER GILCHRIST: Thank you, Madam Chair. Before I ask my question to Mr. Ton-That, because I'm going to come back to you. I certainly want to thank my colleague, Commissioner Jones, for his leadership on this initiative. I think he allowed me to offer some input into this discussion today, and I certainly appreciate the opportunity to do that so, Commissioner, thank you.

My question about training is a little bit different. It is more so geared towards training the models to deal with AI. Can you talk a little bit about that part of it. Because I think -- and I will ask this question in particular with regard to regulation because I think this gets into the

algorithmic side of this that I would like to really understand a little bit better.

MR. TON-THAT: Sure. Thanks, Commissioner Gilchrist. So earlier algorithms regarding facial recognition wouldn't use AI on machine learning and were quite inaccurate. So they would do things like measure the distance between the eyes or look at skin color, really kind of basic things.

But with the advent of machine learning and artificial intelligence, facial recognition has gotten remarkably more accurate. And the way it works when you train an algorithm is you try and find the photos of many different people and different demographics and different poses. And the more data that a model has the more accurate it gets across different demographics.

So over time what we have been able to do is pull millions of photos from the public internet to train our algorithms to be more accurate.

COMMISSIONER GILCHRIST: So if something is disproportionate, does that in some way could potentially disproportionately train an algorithm?

MR. TON-THAT: That's a great question. It's not quite related to the proportions. What we found is the more examples there are of any

demographic or any type of person the more accurate it gets across all those demographics.

So if you look at Clearview's accuracy across in the NIST one to N test, the highest threshold NIST has, white males are at 99.99 percent, Black males at 99.97 percent, white females are at 99.98 percent and Black females are at 99.93 percent. So this wouldn't be possible without the advent of machine learning. You can gather a lot of data to make these models more accurate.

I think the bias that an algorithm has today with the top performing algorithms is, you know, kind of negligible. The flip side is, people always say, even if the algorithm is accurate, does it make policing more biased or less biased. And I think that comes down to the data set you search against.

So some other vendors for facial recognition only search against mugshot data, right?

COMMISSIONER GILCHRIST: Right.

MR. TON-THAT: So what's that going to do? That's going to affect people who have been through the prison system before. Our system searches through data from everyone from the public internet.

So I really do believe that is a way to decrease bias and policing on a systemic level.

COMMISSIONER GILCHRIST: And so from a regulatory perspective, do you think we should focus -- do you think we should think about regulations with regard to regulating the algorithmic side of it or do you think it should be on the end user side?

MR. TON-THAT: I think it's both.

COMMISSIONER GILCHRIST: Yeah.

MR. TON-THAT: We are a proponent of facial recognition regulation. We took it upon ourselves to not sell this data set beyond government and law enforcement. Some states like Virginia have passed laws where you can use facial recognition for law enforcement, but there is a requirement that there is a minimum accuracy level according to NIST.

So I think, yeah, we are very open to regulation. We think it's a good thing. It will build trust with the community, with policing and with the general public.

COMMISSIONER GILCHRIST: Thank you.

CHAIR GARZA: I'm going to jump in here. I see that Mr. Lee, you want to be recognized, and then I have a note that Commissioner Magpantay has a question on the phone. So we don't want to forget him.

COMMISSIONER MAGPANTAY: Thank you.

CHAIR GARZA: Go ahead, Mr. Lee.

MR. LEE: Sorry. I just want to clarify a few things that Mr. Ton-That said about the kind of the AI behind Clearview AI and what is really implicated when you are using publicly scraped information on the internet from social media platforms.

One of the things we have to keep in mind is that not everyone has access to the internet. Not everyone shares photos on the internet. And there are still many parts of the United States that don't have consistent internet access. There are many different kinds of people who don't have social media. The early adopters of these technologies are disproportionately white.

And so when we are talking about publicly scraped data and publicly scraped images, disproportionately it is going to lean, for the fundamental training set and the fundamental training data of these facial recognition systems are fundamentally going to lean disproportionately towards being more accurate from white users than they are for people of color.

And one thing to kind of highlight for Mr. Ton-That's point about the one to N point from NIST

and the training set, so one to N is one to many. There are different kinds of facial recognition searches.

One you could do is like when you are going into TSA, for example, they check your face versus the face on your passport. That's one to one. One to many is searching your face versus millions of images or thousands of images to see if you are the person who -- or to see if there is a match in there.

And I think that is important to contemplate because one of the things that happens is at scale is where the issues lie. So even if you do have 99.9 percent accuracy, right, I don't know, Mr. Ton-That if you would be able to say that your accuracy is the same for Black people as it is for white people.

And that differentiation across scale, hundreds of thousands of images that are being searched that Mrs. Goodwin highlighted that law enforcement is engaging in. Based on those hundreds of thousands of images, there may be in those hundreds of thousands of images, hundreds, if not thousands of people who may be wrongfully identified within those data sets.

And I think that is an important

distinction to make here because we are not just talking about one individual. We are talking about hundreds of thousands if not even millions of individuals. And unfortunately, the Commission doesn't have the information in front of it to be able to say how often law enforcement is using it across the nation in local law enforcement and then also how often the federal government is using this within the context of law enforcement as well.

And so that's just something to keep in mind as we have this conversation.

CHAIR GARZA: Go ahead, Mr. Ton-That.

MR. TON-THAT: I just wanted to clarify a few things. So the NIST one-to-one test, that's the test that also measures the demographic breakdown across the demographics on accuracy. But the one to N test, which is can you pick a photo out of 12 million images, Clearview is still 99.85 percent accurate for that.

So can you imagine trying to go through 12 million images and trying to pin down the right person? It's got a very high level of accuracy.

I do agree with Mr. Lee that getting more information about how law enforcement is using it is really important because that's how everyone here can

learn, you know, the positives and the negatives about it.

So we provide in our technology a way for the administrators to oversee not just the searches that have been done, but general information. How many searches per month? What type of crime were they used again? Were these cases closed or not?

So as a vendor in this space, we are very committed to helping law enforcement get that information so they can report to the public or to GAO and other places than that.

CHAIR GARZA: Yeah. We're still waiting for some information.

I'm going to go to Commissioner Magpantay first and then I will go to Commissioner Adams if that's okay.

COMMISSIONER MAGPANTAY: Thank you, Madam Chair. Glenn Magpantay. Thank you, Mr. Ton-That for your comments. It was really quite illuminating. And, Mr. Ton-That, I really do appreciate your presence here and your testimony.

You just rattled off a couple of percentages for white women, white men, Black men, Black women. Do you have other demographic groups? If you don't have it right now, if you can provide

that to the Commission, I would like to see that as well. Thank you.

MR. TON-THAT: Thanks, Commissioner Magpantay. In this report, those numbers are drawn from there. And they do have other demographic groups and ways to measure things beyond those like country or origin and so on. So I would refer to the NIST report. It's very thorough. And I'm a resource as well if you want to follow-up with me on anything else specific. Thank you.

COMMISSIONER MAGPANTAY: Okay. Thanks.

CHAIR GARZA: Commissioner Adams?

COMMISSIONER ADAMS: Thank you, Madam Chair. Professor Ewert, and I apologize, it's German.

MS. EWERT: You got it.

COMMISSIONER ADAMS: I was very sympathetic to your comment that surrendering biological data to third parties is what you said about these residents. And I'm sympathetic to that concern.

Isn't the horse a little bit out of the barn on this? I mean, do the residents there have, for example, phones with Google and location tracking and heartbeat tracking and all of the other surrendering of information, biological information to

third parties is already taking place?

And how do you square the two -- you are extraordinarily concerned about facial recognition? What do they say about the other biological data they are surrendering?

Ms. EWERT: So this is the crux of the issue. Can people give meaningful consent to the use of FRT in surveillance? And so, you know, someone can choose whether to use a smart phone and how to use a smart phone, can choose whether to participate in the trusted traveler, you know, program for airport access, things like that.

The issue with people like my clients, you know, low-income Americans who are in subsidized housing, I would argue there isn't really an alternative.

So, for example, if you are someone with disabilities and you subsist on SSI benefits as your only source of income, you get $943 a month. And I don't think there is anywhere in the U.S. where on $943 a month you can pay market rent and your utilities and your household products -- I'm leaving food out of that because hopefully folks are applying for SNAP benefits -- you know, transportation and the other things and have a cushion left over so if there

is an economic, you know emergency that you face, you can pay for that as well as your rent.

And so for folks on very fixed incomes, if you are not in subsidized housing, like public housing or Section 8 where your rent goes down when your income goes down, you are at very real risk for eviction.

And what are options for folks if they get evicted from, you know, the market rate housing or even subsidized housing? They might, if they're lucky, would be able to couch surf with family and friends. But that's not reliable. And that also puts their family and friends at risk of eviction if they are renters, you know, they are not supposed to have unauthorized occupants.

The second option, if they have a car, they could live in their car. Not convenient, not easy, not particularly safe. A lot of low-income folks don't have cars.

What's the third option? Going to a congregate shelter. There are a whole host of problems around that. And God forbid you're a woman who has a teenage son because a lot of congregate shelters don't allow boys aged 14 and over to stay with their families. And so where does that leave

you? Outside in an encampment, which is not safe.

And so if you are a person on a very fixed income, subsidized housing is your best bet for staying safely housed. And so I would argue that the consumers who are using this housing, who are submitting to the surveillance and this technology, don't really have a good alternative. And a lot of the regulatory proposals are focusing on consumer consent, you know, can people opt out? Do they understand what they are agreeing to? And that is simply is not an option for my clients who depend on subsidized housing.

I hope that answers your question.

CHAIR GARZA: Commissioner Jones?

COMMISSIONER JONES: Thank you all for your testimony. This has been really constructive. I am sympathetic to Ms. Kinsey's argument that we've got a real challenge because thus far we have overwhelmingly relied on the representations made by departments, agencies, companies, like Clearview even, in terms of anecdotal data and whatever statistics that may be trotted out without an ability as the public to independently corroborate sort of representative data. Obviously, we can all do the anecdotes. And these are compelling anecdotes by the

way. So thank you.

So with that, I wanted to ask you, as the CEO of your company, has Clearview conducted or facilitated and then publicly released the results of any operational testimony of its FRT service as used by law enforcement agencies?

MR. TON-THAT: Thanks, Commissioner Jones. As a vendor, as a company, we are always encouraging our law enforcement partners to share their positive success stories and then also track in a statistic way the results of the facial recognition.

With the training tools right now, it was very easy for any user of Clearview as administrator to go in and generate a report on how many searches, what type of crimes that it solved with it and so on, who is doing the searches.

I think there is more we can do as a vendor. But at the end of the day, it comes down to the law enforcement agencies and their willingness to share. And unfortunately, it's not that many of them who want to be as transparent about how they use it.

And I think some of the reasons are, and I can't speak for them, is they are not always comfortable revealing their investigative techniques. However, I do think that's an area that we are

looking to do more of.

We haven't made any plans for it yet, but we've thought of ideas where we can start collecting more information and help law enforcement track the actual outcomes at the end of the day, for example number of dollars saved, number of arrests made, number of identifications. And we want to help them do that by putting that into our software.

And hopefully if enough of these agencies who are our clients end up doing it, we could probably generate a more comprehensive report that covers across all those agencies. But I think a lot of it comes down to the unwillingness for various reasons of law enforcement to get into more detail.

COMMISSIONER JONES: And so I want to be clear for everyone listening that that was a no in response to my question.

And so but you guys are touting an oversight function. So technically you do have the data. It's just that it's up to the agencies with respect to whether they want to release that data.

And are you contractually prohibited from releasing sort of data that is not specific to the agency but just sort of --

MR. TON-THAT: Yeah, I would say that we

store and house their data. But we don't have direct access to it. That would be a violation of their expectation around sensitive criminal investigative data to share that without their consent.

COMMISSIONER JONES: Yeah, okay. I mean, I just wanted to ask the question.

MR. TON-THAT: Thank you.

CHAIR GARZA: Chief Aguilar, and then I know we have a question over the phone from Commissioner Kirsanow but I will go ahead and let Chief Aguilar speak.

MR. AGUILAR: Thank you, Chair. Just a quick follow-up to your question, Commissioner. So I don't have the exact data. When I looked at it, I believe it was based off of our 2022 data, but we are looking at -- because we are one of those agencies that has been very transparent. Everything from our policies to our use of the technology in criminal cases.

At last check, we were at about a 40 percent rate of positive identifications. Now, that doesn't mean that we had a 60 percent false metric, right? Because there are a lot of variables involved here.

Number one, it relies on the detective or

the officer that requested the search to our real-time crime center to report back, which we wish always happened. It doesn't always happen. But to report back and say, yes, that match that you sent me was in fact positively identified as a suspect, as a victim, as a witness in this case.

But, again, you know, we're looking at variables such as the -- we have a probe photograph that gets run through the system, and there is no return because there is no photo on the other end of the database. But our positive ID rate is roughly 40 percent.

COMMISSIONER JONES: So as I understand your testimony just now, you're running a search. There is a hit. And at least based on what you just said, only 40 percent of the time does that turn out to be inaccurate.

MR. AGUILAR: No. Because, again, many variables, right? So now the most important thing, right, you know, in our search results that get sent to our detectives or the officer that's requesting that search, the most important part of our policy is printed in bold letters on the top of that hit, which is this is to be treated only as an investigative lead and not as probable cause.

So now that detective has to go out and do their due diligence, for example, putting a photograph of that suspect into a photographic lineup. Well, now they go to an eyewitness and the eyewitness can't identify, right? He doesn't have an accurate enough recollection. We can't find anybody to accurately identify that potential suspect. The case could go cold after that if there are no other leads.

COMMISSIONER JONES: So I understand that perfect, which speaks to the importance of having an actual human being and a policy that says this match is not going to be treated as probable cause for example.

But it is alarming that before human intervention at the end of that, that hit turns out to be accurate to the extent of 40 percent. That speaks to, I think, the fallibility of the software.

MR. AGUILAR: Well, if I could -- I think that we may agree on this more than it might seem. I think that actually speaks to the strength of our practices, right? That we are not running out and making an arrest just because an algorithm tells us to do so.

The robots haven't fully taken over yet so the humans are still in charge. I think that it just,

again, 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, right, physical testimony or circumstantial evidence as we can to either make this case or not.

And so I'm quite happy that, you know, 60 percent of our searches do not result in an arrest. I think that that's more a testament to the fact that we are not using the technology indiscriminately.

COMMISSIONER JONES: And which software are you using by the way?

MR. AGUILAR: We use Clearview AI, and we use a program that is run out of one of the counties in Florida, the Pinellas County Sheriff's Office, that shares their database with all Florida law enforcement agencies. The program is called FACESNXT.

CHAIR GARZA: Do you have a comment?

MS. KINSEY: Yeah, I just wanted to follow-up on Commissioner Jones's question because I think it makes -- the colloquy there is kind of the baseline point I was trying to make today which is that without regulation, we are not going to get the kind of transparency and information that we need.

So I think the response to your question

about operational testing that Clearview does was basically, well, that's up to the agency. So you're going to continue to get this kind of buck passing. There isn't regulation that requires it, that sets these responsibilities out there.

And we can't rely on a responsible agency like Miami PD to set its own rules that, you know, might need to be the rules for all agencies to follow. And that we can't just ask permission for these things. We need to regulate these technologies.

CHAIR GARZA: Well, I appreciate that comment and am in agreement that the heart of this is really about finding some kind of policy to ground us and making sure that we are protecting people's civil rights and civil liberties and to things as basic as their freedom and their housing.

I know we have one question on the phone. That will be our last question for this panel. Unfortunately, we can't be here all day. Commissioner Kirsanow?

COMMISSIONER KIRSANOW: Thank you, Madam Chair, and thank you to the witnesses. This is for anybody. But I would like to direct it first toward Chief Aguilar.

Do you maintain data related to the

percentage of false positives by eyewitnesses versus the percentage of false positives related to facial recognition technology?

MR. AGUILAR: So no. We do not maintain data anytime where -- if I understand the question correctly, where there has been a face recognition match and the case has, I guess, through other means identified another suspect. Was that the question?

COMMISSIONER KIRSANOW: Right. And how does that compare between facial recognition technology versus eyewitness testimony or eyewitness recognition?

MR. AGUILAR: So, again, we don't keep data specifically on either one of those two. But what we do know from the research and much of the testimony that we've heard is that eyewitness testimony is in itself fraught with problems.

But no. We don't track how many times somebody doesn't identify somebody. And, again, there are many variables there, right. But the short answer is no, we don't collect data on either.

COMMISSIONER KIRSANOW: Thanks, Chief. And my follow-up is to anyone who has data or an answer. And that is are the percentage of false positives related to race comparable or wildly

disparate from percentages of false positives related to any other protected class, such as sex, age, national origin?

MR. TON-THAT: Yeah. Thanks, Commissioner. If you look at another thing that is really important for facial recognition, it's image quality.

So NIST also tests visa photos versus mugshot photos versus what they call border photos, which is photos at the border from different angles. And they also test what they call wild photos, which are photos from all different types of angles.

If you look at the differences between accuracy, for example between wild photos and mugshot photos, that is much, much greater than, say, accuracy between Black men and white women. So there are other parts of the NIST report that are quite thorough that go into the types of photos that are being tested against.

CHAIR GARZA: Mr. Lee.

MR. LEE: I think that's a slight misinterpretation of the data. I would disagree with that finding.

I would argue that even if you have a 99 percent accuracy, right, it's 1 in 100 people are likely to be misidentified. And it's just the

likelihood of that one person being of color or not.

And to answer your question, Commissioner, if you look across the NIST one-to-one variables, consistently you will see the biggest difference in false match rate is between either East Asian people and Black people or white people and Black people, particularly amongst Black women ages 65 to 90.

MS. KINSEY: Can I respond to the eyewitness question?

CHAIR GARZA: Sure.

MS. KINSEY: So I just -- I feel like this has already been brought up a couple times today. And I think the bit of kind of a kind of false premise that facial recognition and eyewitness ID are opposite sides of the same coin because facial recognition is a process that involves human reviewers at multiple points in the process.

You have an officer reviewing the results and then you often have an officer taking those results and having another eyewitness review those results. So you are not separating out the issues of eyewitness ID from facial recognition technology. There is actually the possibility that they could compound and amplify the issues that you see with eyewitness ID. And there have been studies that show

that facial recognition technology because it does a good job of pulling out similar looking look-alikes, so not the actual person but the most similar looking people, it makes the task of the human reviewer reviewing those results more difficult because we are not good at distinguishing among unfamiliar faces.

So I think we do definitely have a need for data on this. You know what are the rates of eyewitness ID and accuracy? What does it look like when you combine that with facial recognition? But considering them as two separate cases, I think, is not accurate when you think about how facial recognition actually works.

CHAIR GARZA: Thank you for that. That was kind of going to the point I was making earlier about how you still have people interacting with the system, with the technology itself.

So we are going to have to leave it there. We are at time. Thank you all, each of you, so much for your testimony. We appreciate you making the time to be here. And we are going to take a brief break and reconvene at 11:35 with our second panel.

(Whereupon, the above-entitled matter went off the record at 11:29 a.m. and resumed at 11:47 a.m.)

PANEL 2: FEDERAL GOVERNMENT UTILIZATION AND SAFEGUARD IMPLEMENTATION OF FRT

CHAIR GARZA: Hello. We're now going to come back to order. It is 11:47 a.m., and we're going to go ahead and proceed with our second panel where will examine the Federal Government Utilization and Safeguard Implementation of Facial Recognition Technology. Each panelist will have seven minutes to speak and following the conclusion of the panel presentation, again, Commissioners will have the opportunity to ask questions within the allotted period of time, and I will go ahead and recognize you Commissioners who wish to speak. Of course, I'll strictly enforce the time allotments given to each panelist to present his or her statement and unless we did not receive your testimony until today, again, you may assume that we have read it, so please summarize it. We'll appreciate that. That way you can make the best use of your seven minutes.

Panelists, please notice the system warning lights that we have set up. When the light turns from green to yellow, that means two minutes remain. When the light turns red, panelists should conclude their statements so you do not miss cutting me off mid-sentence. And my fellow Commissioners and

I will do our part to keep our questions and comments concise.

And in order in which they speak, the panelists are Peter Mina, Deputy Officer for Programs and Compliance, U.S. Department of Homeland Security, Office for Civil Rights and Civil Liberties; Arun Vemury, Senior Engineering Advisor, U.S. Department of Homeland Security, Science and Technology Directorate; Diane Sabatino, Acting Executive Assistant Commissioner, Office of Field Operations. U.S. Customs and Border Protection; Jason Lim, Identity Management Capability Manager at the Transportation Security Administration.

And I'm going to now ask each of you to raise your right hand to be sworn in. Will you swear and confirm that the information that you are about to provide us is true and accurate to the best of your knowledge and belief?

Affirmative from all.

Mr. Mina, you can go ahead and begin.

MR. MINA: Good morning, everyone. Chairwoman Garza, Vice Chair Nourse, and members of the Commissioner, thank you for the opportunity to speak today about the Department of Homeland Security's use of biometric technology and data

responsibly in support of the Homeland Security mission while preserving and protecting civil rights and civil liberties. As the Chairwoman said, my name is Peter Mina, and I am the Deputy Officer for Programs and Compliance with the Department's Office of Civil Rights and Civil Liberties.

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. Face recognition technology can serve as an important tool, and it is vital that these programs use the technology in a way that safeguards our constitutional rights and values. The policies and procedures we follow ensure that the Department's use of this technology is free from discrimination and in full compliance with the law ensuring that we retain the public's trust.

The Department's broad and diverse mission results in millions of interactions with individuals each day. It is critical that DHS utilizes face recognition technology responsibly. I hope this perspective further informs your deliberations rounding out your understanding of the many equities, including individual rights that DHS must consider

whenever the department takes action, especially with technology and data that has a very real impact on individuals.

I'd like to next focus a little bit on something that Dr. Goodwin mentioned in her testimony, which is our Facial Recognition and Face Capture Directive which was recently issued in September of last year. This Directive 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.

And so I want to walk through a few of the key points in the Directive. This Directive prescribes several key points. It dictates that all use of facial recognition and face capture technologies will be thoroughly tested to ensure that there is no unintended bias or disparate impact in accordance with national standards. It directs the review of all existing uses of this technology and to conduct periodic testing and evaluation of all systems

to meet performance goals. It requires that U.S. Citizens be afforded the right to open out of face recognition for specific non law enforcement uses.

It prohibits face recognition from being used as a sole basis for any law or civil enforcement-related action, and it establishes a process for Department oversight offices including the Privacy office, my office, the Office of Civil Rights and Civil Liberties, 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.

And so this Directive was a vital step forward for the Department in establishing a framework for proactively assessing the technologies being utilized and ensuring they're being employed responsibly. Wholesome consideration by my office, operational agencies and offices, DHS leadership and others is critical to ensure we get it right from the beginning and protect the rights of the individuals we serve and the viability of DHS operations. Operators, researchers, civil rights advocates, and policy makers must work together to prevent algorithms that are leading to racial, gender, or other impermissible biases in the use of face recognition technology.

Successful and appropriate use of all biometric technology, including face recognition, requires ongoing oversight and quality assurance achieved through a close relationship between operational users and oversight offices such as CRCL. And you see that, I think, by the representation on the panel today. It is really a partnership across the Department, and that partnership is critical to achieving this critical mission.

And so again, as I mentioned, when deploying biometric systems, civil rights, civil liberties and privacy must be integrated into their foundations, and that's really how this works most effectively is to get involved early and often. And so CRCL has been and continues to be at the forefront of this engagement with DHS agencies and offices to ensure that the DHS use of face recognition is consistent with civil rights and civil liberties, law, and policy. We provide advice and oversight to the Department's efforts to ensure this 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.

And so I can give a comprehensive list of

every factor that we consider when we look at facial recognition technology, but I want to highlight a few things for the Commission. So obviously, one of the main things we look at is discrimination. Biometric technology, either in their design or use, can result in impermissible discriminatory impact, and the presence of algorithmic bias has been highlighted in recent U.S. Government analysis. We've been talking a lot about the NIST report. We've looked at that as well. And then also that NIST report -- you know, while there is a noted substantial bias or substantial demographic effect in many algorithms, the NIST report also highlights the demographic differentials are smaller or undetectable with more accurate, high performing algorithms in certain applications. Even when using such high performing algorithms as DHS does, testing and validation must be a constant in the operational life cycle.

The next thing I want to touch on which was also mentioned in the first panel is scale. With certain biometric modalities, a non-trivial percentage of the population cannot present suitable features to participate in certain biometric systems. For example, many people have fingers that simply don't print well or a disability which would limit their

participation. Even if people are unable to be fingerprinted, for example, who represent one percent of the population, that may translate into a massive inconvenience and suspicion for that minority. The same scaling issues are present when using face recognition technologies making it critical that we identify potential matching issues and address them quickly.

The other thing I want to highlight is perception. While we need to guard against actual and perceived bias in biometric systems, we need to address perceptions that biometrics the Department collects for legitimate reasons are being used to conduct lawful surveillance -- unlawful surveillance -- excuse me -- or tracking individuals. DHS has a responsibility to actively promote a common understanding of the technology and the Department's use and non-use of it. CRCL engages with stakeholders in order to provide feedback to the Department and agency leadership regarding the impacts or consequences of policies, programs, activities, and initiatives.

And then lastly, there's redress. Individuals must have an opportunity to correct both their biographic and biometric information so that

incorrect biometric matching or adverse consequences can be effectively and timely challenged and database corrected. In addition, CRCL, as I mentioned before, has an established complaint process to investigate allegations of violations of civil rights and civil liberties.

And again, one of the things that we look at is looking forward, how we get involved in those projects, how we get involved from the ground up. And then again, as those features and projects develop, we're going to remain engaged with advocates, technologists, and our operational partners to ensure the civil rights and civil liberties protections are both effective and sufficient.

And thank you so much for your time. I look forward to taking your questions.

CHAIR GARZA: Thank you so much, Mr. Mina. We're going to now turn to Mr. Vemury. You can proceed.

MR. VEMURY: Good morning, Chairwoman Garza, Vice Chairman Nourse, and members of the Commission of the Civil Rights and Civil Liberties. I'm honored to be before you today.

My name is Arun Vemury and I'm a Senior Engineering Advisor at the Department of Homeland

Security, Science and Technology Directorate. I serve as the Senior Advisor specifically for biometric and identity technologies. In this role, I am responsible for identifying research needs and coordinating the efforts among multiple international experts on developing technologies to help close different capability gaps for different missions that are supported by the Department.

I also provide leadership to perform testing and evaluation of cutting edge, new technologies including facial recognition to make sure that we have appropriate information to understand how the technologies work, their capabilities, and their limitations.

I've worked in the space of biometrics for more than 20 years.

In 2003, Congress established the Science and Technology Directorate as the research and development arm of the Department of Homeland Security. The Undersecretary for Science of Technology serves as a Senior Advisor to the Secretary of Homeland Security and S&T conducts research, development, tests, and evaluation of the new technologies and capabilities. We work on science that strengthens the technologies and capabilities the

Department requires to help ensure the security and prosperity of our people. Our work on biometric and identity technologies includes facial recognition, and we apply a rigorous and deliberative process to research, test, and evaluate these technologies to inform components of how the specific technologies work in the specific use cases that they are operating in.

Facial recognition technology is relatively easy to use but has not always been accurate. Recent advances in machine learning have enabled some commercial face recognition technologies to make dramatic gains in accuracy. These technologies hold immense potential to help improve the effectiveness of different DHS operations. However, realizing the potential operational gains also requires careful analysis and planning as performance and machine learning base capabilities are affected by multiple factors.

By some measures, face recognition technology is among the most carefully-tested AI technologies, and a significant portion of what we've learned has actually been gained through support from DHS S&T. DHS S&T funds face recognition research, testing and evaluation through distinct channels

including the National Science Foundation Center for Identification Technology Research, which performs early stage research on biometric and identity technologies. We also co-fund the National Institute of Standards and Technology Facial Recognition Technology Evaluations. They changed their acronym recently. I keep wanting to say the old one. –This work focuses more on biometric algorithm testing, in particular.

And then we also, importantly, establish something that's specific and unique to the Department. We established the Maryland Test Facility, a test laboratory that performs applied research and carries out targeted evaluations of integrated end-to-end biometric capabilities, so not just an evaluation on the algorithm. We look at the process. We look at the cameras. We look at all the different software that are integrated throughout the entire process including the portions that require human decision making.

This portfolio allows us to answer key questions about facial recognition technology to inform and advise DHS and its operational components on mission effectiveness and answer questions on performance to inform oversight. The performance of

facial recognition technologies is determined by multiple subsystems. Errors can be made anywhere in the process from the camera to the face detection software, image quality systems, liveness checking, to the facial recognition algorithm, or even the decision logic that determines whether the system assesses that a person may be the same person in two different photos.

Technology tests carried out by NIST have shown the top performing facial recognition algorithms make few errors on previously acquired faces. However, having a top-performing facial recognition algorithm alone does not guarantee accuracy and equitability of the technology and operations. Assessing a technology within the specific use case requires scenario testing and evaluations in operations. Testing performed at the Maryland Test Facility simulates full facial recognition capabilities in simulated use cases informed by DHS's operational needs, and they're complemented by operational evaluations.

DHS works in collaboration with our DHS operational components to make sure that we are developing tests that are actually indicative of real world operational processes. We have applied our

research and testing evaluation to multiple government and commercial systems. The work that we've done and the findings that we've presented have also been published in peer reviewed scientific publications, at conferences, and technical papers. We've also briefed out our results and findings to industry and academic associations to help inform innovation so that commercial and other academics can help develop new technologies that address the capability and limitations that we find through our testing.

Through comprehensive assessments, we work to inform and empower the Department to help improve their ability to identify accurate, effective, and fair technologies that align with their statutory and regulatory missions.

We are also actively engaged in leading the development of international standards aimed at establishing guidelines for the effective and responsible use of the technologies. Standards are really important because they help with the assessment of facial recognition technologies, because they ensure that different stakeholders have a common understanding of terms and metrics. To help standardize the way we talk about biometric system performance across demographic groups, we are also

leading the development of a new international standard known as ISO/IEC 19795-10. There will not be a quiz at the end.

Through efforts like this, we seek to promote transparency, accountability, and equitability of these technologies. The DHS Directive on face recognition and capture technology published in September of 2023 requires DHS S&T to perform evaluations of new facial recognition capabilities. We plan to ensure that these deployed systems with the same rigor we've evaluated in research and commercial systems before. Our recent assessments of a TSA credential authentication technology for system effectiveness, efficiency, and equitability serves as an example of this approach. And we -- as part of this process, we've applied both -- comprehensively laboratory scenario and operational evaluation so we get a more holistic picture on the overall performance of the system, not only to help TSA identify ways to improve the performance of their systems, but also to inform oversight.

In conclusion, the responsible use of facial recognition technologies by federal agencies requires a concerted effort encompassing rigorous research, inclusive testing methodologies, and

international collaboration with experts, appropriate guidance as well as appropriate policies to help ensure that we are doing it effectively. By adhering to these principles, we ensure that the technology serves not only a use for security but also safeguarding privacy, civil rights, and civil liberties for all Americans.

Thank you for the opportunity to speak to you and I welcome any questions you may have.

CHAIR GARZA: Thank you, Mr. Vemury. We're going to now hear from Ms. Sabatino. Please proceed.

MS. SABATINO: Chairwoman Garza and members and staff of the Commission, thank you so much for the opportunity to speak today on behalf of U.S. Customs and Border Protection's efforts to better secure our Nation and facilitate lawful travel through facial biometric comparison technology. By leveraging biometric identification capabilities, we have essentially automated a previously manual process to verify the identity of travelers entering the United States. In building the Traveler Verification Service, known as TVS, which provides back end facial biometrics matching, we've implemented facial biometrics at all ports of entry supporting

international air arrivals including all of our pre-clearance locations. We've established facial biometrics at 40 seaports and all of our pedestrian lanes at both the Southwest border and Northern border land ports of entry.

Since the outset in working and using facial biometrics, we've worked closely with our partners here at the table but also with the National Institute of Standards and Technology to ensure high performing algorithms for matching and immediately saw a high rate of successful matches. A NIST test earlier this month showed the NEC algorithm, which we use, performed with an accuracy rate of 99.88 percent, and our data analysis also indicates there is virtually no discernible differential with respect to demographics, with high technical match rates across the globe.

We achieved the accuracy and speed of matching by building galleries of existing traveler photos from passports, visa applications, and prior Department of Homeland Security encounters. So if a traveler cannot be matched by our biometric facial comparison technology, they simply undergo, I should say, a manual identity check consistent with existing requirements for entry into the United States. And to

date, more than 470 million travelers have been processed using biometric facial comparison technology allowing us to biometrically confirm more than 325,000 overstays in the U.S. and identify more than 1,900 imposters attempting to enter the U.S.

But privacy is not an afterthought and travelers should not have to sacrifice their privacy for processing efficiency or convenience. As we implement any new technology, the privacy protections and data security are built in from the very beginning of developing a program. And our primary use of facial biometrics comparison technology is at a time and a place where an individual would normally expect to present themselves for identity verification. We inform travelers through various channels regarding when photos will be taken for identity verification purposes and whether they can opt out if they're eligible to do so.

And furthermore, we conduct ongoing public awareness campaigns and provide details through privacy impact assessments and notices. Continuous testing and evaluation remain integral to enhancing our capabilities and ensuring that our frontline personnel have the best tools possible to increase their focus on situational awareness to better protect

our borders. TVS, I mentioned, our facial biometric matching system, is just one of a number of tools that we use to inform our frontline officers in order for them to make the best decisions. Our officers remain our most valuable resource in the entire process.

CBP faces an incredibly dynamic and ever-evolving threat landscapes, so ensuring that our frontline personnel have the right tools to do their jobs is of paramount importance to us. And while facial biometrics comparison technology is critical to our operations, many other tools, including mobile applications, intelligence, nonintrusive inspection systems, and canine operations are also in place to secure our border. However, nothing will replace the keen intuition and the skills of the officer making the decision. They will always have the final say in the inspections next steps with a traveler. But biometrics has and will remain another tool in our tool belt to use.

And today we continue to look to industry and other foreign partners as well as U.S. entities, again, none more important than my colleagues here on the panel, to identify best practices. One example would be the Biometrics Institute. It's an international organization comprised of government,

industry, and academia that's established the good practice framework and expert reference guide for designing and implementing biometric systems and programs. So not only have we shared our best practices with the Biometric Institute and through other international forums, we also have learned through these international engagements, because we want to ensure that we have visibility and the opportunity to continually improve and help establish high global standards. We certainly look well beyond the work we do every day to ensure that we avoid blind spots and potential bias due to the limitations of our geographic footprint as well as our stakeholders.

And moving forward, we're going to continue to work closely with those key stakeholder including NIST, Congress, industry, and our travel partners to seek the most innovative technologies, streamline our business processes, and strengthen our border security operations.

So thank you for the opportunity to speak with you today, and I look forward to answering your questions.

CHAIR GARZA: Thank you, Ms. Sabatino. Mr. Lim. You can proceed.

MR. LIM: Good afternoon, Chairwoman

Garza, members and staff of the Commission. It's really an honor to be here, and thank you for this opportunity to engage with you. Today I'm Transportation Security Administration's Implementation Official, Recognition Technology to include security and passenger experience at our checkpoints.

So kind of echoing what the previous panelists have said, more than any other type of technology, I believe it's important to understand the particular use case when talking about face recognition; in other words, how is it being used? The answer to that question really drives everything about how you implement the technology and the processes and policies throughout it.

So at TSA, facial recognition is not used for surveillance, investigation, or any other law enforcement uses. TSA has a very specific and limited use cases, has well-defined and constrained to a single point of interaction at the checkpoint; that is to confirm who you are before you enter into the checkpoint for screening.

A critical step to verifying your identity, is ensuring that the passenger's face, the live face, matches the ID photo that they just

presented. So this means trying to match a small photo of a stranger on an ID to a person you're seeing for the first time. So repeat this for up to 200 times an hour, extrapolate this to about 2.5 million times a day across a TSA enterprise. And this traditionally has been manual, this process, so in the past few years, TSA has been automating the specific step in the process in order to enhance passenger experience and improve identity verification, which is a linchpin to TSA's risk-based security regime.

As we have done this, we have put privacy and civil rights as our core design principles. This has led to a suite of privacy-enhancing functionalities and processes. For example, one, your live photo as well as the ID scan are deleted upon match. We don't keep it. Your photo capture, the matching that happens and the deletion of that photo and the ID scan all happen at the edge. By that I mean it happens on that local machine that you're interfacing right then and there without any of the biometrics data being sent upstream to any centralized, you know, back end databases.

Our device's camera only takes the photo when there's a specific action to trigger the photo capture. This is called active capture, and it's a

feature that we designed. That means that the camera is not constantly on and it's scanning the environment for some face to come into the field of vision. There has to be an explicit action for you to turn on the camera and take the picture.

And most importantly, you 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 nearby our devices to inform the passengers of their right to opt out.

And additionally, you know, we have integrated this opt out language, right, 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.

The match result is presented to the TSA officer as a part of the larger set of data for the officer to use his or her experience, training, and contextual judgment to determine that someone is who they say they are. In other words, human judgment is always in the loop and the last word on any security

decision.

And finally, we have published public impact assessments that lay out in detail how we have implemented this technology and what we do with your data. In fact, we have published multiple privacy impact assessments, held several roundtables with privacy and civil rights advocacy groups over the years as we explored this technology.

It's also critical that our facial recognition technology performs equally well across all demographics and lighting conditions at different airports. This is key when you're talking about a very diverse population of 2.5 million passengers every day. So therefore, we worked with our DHS Science and Technology Directorate colleagues, especially with Arun Vemury, for his lab to independently test our specific system end to end across multiple dimensions. This means not just a matching algorithm as he pointed out but also the camera, how we process the image, how the matching happens, the usability, and the user interface and human factors and all those different dimensions to specifically understand any performance differentials across age, gender, and race.

But we're not satisfied with just one

test. We have engaged in continuous testing and post implementation reviews including, as the previous panel pointed out, testing in real world traditions in our operational checkpoints. In fact, both DHS S&T and TSA's own independent test authorities have performed multiple tests and analyses on our device over the years. And further, we have recently expanded our analysis, you know, for performance differentials across demographics groups with a larger sample size, with more granular demographics classification to continually ensure that our technology does not perform less accurately for specific groups.

In addition to the privacy impact assessment, we have also published the TSA biometrics roadmap back in 2018, TSA Identity Management roadmap in 2022 that lays out our overall approach to improve identity security using biometrics. And we are very happy to share these with the Commission.

Moving forward, please be assured that TSA will continue to work closely with key stakeholder and partners to continually improve our security while enhancing the passenger experience and safeguarding your privacy and civil rights and civil liberties. Thank you for the opportunity to speak today. I look

forward to answering your questions.

CHAIR GARZA: Thank you so much. Thank you, Mr. Lim and the rest of the panelists. I do want to acknowledge that we have -- before I open it up for questioning -- that we do have Vice Chair Nourse on the phone; is that correct?

VICE CHAIR NOURSE: Can you hear me?

CHAIR GARZA: Yes. We can hear you. Okay. Great.

VICE CHAIR NOURSE: Thank you.

CHAIR GARZA: Wonderful. So I'll go ahead and open it up for questions if anyone would like to start. Commissioner Adams?

COMMISSIONER ADAMS: Thank you, Madam Chair. My first question is for you, Mr. Mina. It's a structural question related to some concerns voiced at the beginning of this presentation today. You're at DHS, right, and you have guidelines, presumably, related to these issues in place now?

MR. MINA: Yes. I'm sorry. Yes.

COMMISSIONER ADAMS: Okay. Were -- if DOJ, Department of Justice, were to interface with your Department either through the Civil Rights Division or Office of Legal Counsel and have guidelines that were inconsistent with yours or

different than yours, theirs would -- ultimately, their direction would replace yours, correct?

MR. MINA: So while we certainly get -- and us, I don't want to speak for the Department of Justice, but I think that while we certainly get guidance from DOJ and we coordinate, we do have distinct authorities and I think that there are reasons why our Directive would co-exist with the DOJ Directive on facial recognition, for example.

COMMISSIONER ADAMS: Is that because their view already is consistent with yours and --

MR. MINA: Again, I don't -- I just don't want to speak for DOJ at this point. I think that that's something that certainly we would work closely, as you mentioned, with the Civil Rights Division to coordinate, but I think that's -- again, I think that our Directive issued in September of last year, you know, stands on its own as it relates to our use case. I think that's the important part.

COMMISSIONER ADAMS: When you say stand on its own, this means wholly developed by DHS?

MR. MINA: Right. Wholly developed by DHS, right.

COMMISSIONER ADAMS: Okay. My next series of questions is for Ms. Sabatino. You talked about

the biometric capture. I assume since this is a facial recognition hearing, you refer primarily to a facial capture, right? I mean I just don't know.

MS. SABATINO: Our facial biometric comparison technology uses a facial recognition algorithm, but it is a service that builds galleries based on advanced passenger information. So it is more comprehensive than the algorithm itself and why --

COMMISSIONER ADAMS: Okay.

MS. SABATINO: -- we refer to it as such. But it is facial.

COMMISSIONER ADAMS: But there's like a harvesting process of facial images I assume. For example, does it happen at an administrative arrest? Do you do biometric capture then?

MS. SABATINO: So how we leverage, our business use case, the most significant use case is for arrivals to the U.S. And there are two means to do that. In our air and maritime environment, we receive air passenger information from commercial carriers. And leveraging that air -- that advanced passenger information, we will then build galleries either establish U.S. passport photos, visa photos, or prior DHS encounters and build that gallery and match

as the individuals arrive based on the documentation they present and then the image that they present.

In our land border environment, we do not build galleries. We do a one-to-one matching with the document that the individual presents, with the RFID that's read or when we swipe the document.

COMMISSIONER ADAMS: Okay. So I understand the passenger, like a Dulles United Airways. But what I'm asking about specifically is during an administrative arrest, does DHS capture a facial image, yes or no?

MS. SABATINO: So any individual that we take into custody, we would capture an image of the individual.

COMMISSIONER ADAMS: Okay. What about an apprehension?

MS. SABATINO: So I'm not sure the context of apprehension, you know, in terms --

COMMISSIONER ADAMS: Well, I can --

MS. SABATINO: -- what specifically --

COMMISSIONER ADAMS: -- DHS has a glossary helpfully on the internet, and they make a distinction between administrative arrests and apprehension. I was wondering if that's something you also capture the facial recognition or facial imagery.

MS. SABATINO: Any time an individual is taken into custody.

COMMISSIONER ADAMS: What about an administrative encounter without taking into custody?

MS. SABATINO: An administrative encounter as defined by -- any individual that arrives, foreign nationals -- U.S. citizens can opt out, but any foreign national that arrives at a U.S. port of entry, we capture their image.

COMMISSIONER ADAMS: Okay. What if they walked across not at a port of entry, what if they -- you administrative encounter with somebody who did not arrive at a port of entry?

MS. SABATINO: Are you referring to individuals who arrive in between the ports of entry?

COMMISSIONER ADAMS: Or show up in San Antonio, for example, and you have an administrative encounter, do you take facial data at that point?

MS. SABATINO: Okay. With respect to individuals in the interior, it's not where the Office of Field Operation operates. We operate at the ports of entry. Our colleagues in the Border Patrol in between the ports of entry, individuals crossing the border essentially is where we would encounter them, which means arriving at an airport via a crew ship,

small vessel, or vehicle, or pedestrian crossing.

COMMISSIONER ADAMS: What about asylee, do you capture facial recognition for an asylee?

MS. SABATINO: Yes. Any individual that is arriving at a port of entry.

COMMISSIONER ADAMS: Diplomatic passports, do you --

MS. SABATINO: Diplomats are exempt in certain instances, yes.

COMMISSIONER ADAMS: All instances or just certain?

MS. SABATINO: It's certain categories. I believe it's A's and G's.

COMMISSIONER ADAMS: Okay. At book in processing, when you book them into a detention facility, is facial data captured then?

MS. SABATINO: I would have to defer to ICE Enforcement and Removal operations.

COMMISSIONER ADAMS: Are you familiar with the DHS SAVE database, Systematic Alien Verification for Entitlements, database?

MS. SABATINO: That is not a database that we employ.

COMMISSIONER ADAMS: Okay. That's all I have.

MS. SABATINO: Thank you.

CHAIR GARZA: I do have a quick follow-up question as somebody who lives on the border and crosses the border all the time in Texas. We just heard that TSA does not keep those images. Does -- is that the same for when somebody is crossing a port of entry, they're an American citizen, they have their image captured, does that go into a database? What happens with that image?

MS. SABATINO: So U.S. citizens, the photos are deleted well within 12 hours of them crossing the border, retained potentially just for evaluation, but they're often deleted long before the 12-hour mark. Foreign nationals, NIST goes back to when we implemented US-VISIT back in 2004. The images are not retained in the Traveler Verification Service. They are transmitted over to the IDENT system where they're retained, I believe, the timeframe is 75 years.

CHAIR GARZA: Okay. And I do -- I just ask one other follow-up question of our DHS folks about mandatory training for FRT use by staff. What kind of training does that look like?

MS. SABATINO: I think certainly in any -- and treating the facial biometrics like we would treat

any data point that, you know, we have in our systems, we have overarching training with respect to privacy, system security, cybersecurity, protecting classified information but also, you know, inclusion and diversity are all like overarching training.

With respect to facial recognition technology, we have based on a GAO report, I believe, that was completed last year working through the development of some training that we expect to have implemented by April '24, so in the next several weeks, hopefully, have that implemented and up and running.

I think in terms of as a tool that we use, what we focus on with our officers and the teams that use the biometric facial comparison technology, like any other data point that we have, the, you know, primary consideration for them is that is not the sole reason that an individual is subject to any further actions with respect to their inspection itself, that we have multiple data points, and the most important one being the interview with a frontline CBP officer to make a determination.

CHAIR GARZA: Thank you. Somebody else want to answer that? Mr. Mina.

MR. MINA: I just wanted to -- thank you

Chairwoman. I just wanted to highlight the policy piece that sort of also supplements that. So like for -- and these were also cited in the GAO report but for example, I know there was a discussion earlier about First Amendment protected activity. And so there is a memorandum that's been issued and it's more general guidance. Granted it's supposed to be more specific training, but it does also touch on use of biometrics, which is, you know, a memorandum related to collection interface and related First Amendment protected activity issued in 2019.

And then also just our general policies on discrimination in law enforcement and screening activities I think also sort of touch on these issues as well.

CHAIR GARZA: I'm going to recognize Commissioner Magpantay.

COMMISSIONER MAGPANTAY: Thank you. And first, thank you for being here and thank you for your service. No, really. It's actually delightful to hear this presentation which I'll -- I have a question about TSA and the optionality of the photos. I thought it was optional, and isn't not optional, and what -- don't travelers have the opportunity to know that they have the option not to have their picture

taken?

MR. LIM: Yes. I thought --

MR. VEMURY: Yes. He testified --

COMMISSIONER MAGPANTAY: Where does that happen?

MR. LIM: It happens right there at the checkpoint when you actually encounter -- it's the first time you encounter TSA at the point we call travel document checker. And that's where our device is to actually confirm your identity, and you have signages nearby or along the queue as you wait. We also have language on the screen itself that you will see when you actually step in front of the machine that says you have a right to opt out or something to that effect.

COMMISSIONER MAGPANTAY: So maybe my question would be better placed if I said, you know, I just came from the airport and I had no sense that that was available. So perhaps it's an implementation question, and I'm happy to take many pictures of TSA agents and share them with you where that is not known. I hear the testimony.

MR. LIM: Right -- right.

COMMISSIONER MAGPANTAY: But I can assure you having flown to many places. Second, can I just

ask are notifications available in other languages besides English and Spanish? Or actually, other languages besides English?

MR. LIM: Yes. So there are signages in English and Spanish. We also have handouts in English and Spanish but not other languages other than that. So --

COMMISSIONER MAGPANTAY: Where are they located?

MR. LIM: So really, operations -- well, checkpoints are so different from each airport, but the guidance is when you implement this technology, as you say, you know what, this technology is actually an operation deployment right now, so it's not everywhere. So it's actually not across -- it's not fully saturated across the TSA enterprise. So there will still be gaps, right, where some airports you encounter, some airports you won't.

Having said that, the signages are located along the queues as you flow into the checkpoint near the machine, hopefully nearby to the signs. And also the signage itself is a digital sign that's on the screen that's attached to the machine.

COMMISSIONER MAGPANTAY: Sure.

CHAIR GARZA: Commissioner Jones?

COMMISSIONER JONES: Thank you, Madam Chair. I'll echo my colleague's observation from his own experience that I have never felt like I had the option to not have my photo taken.

But I wanted to ask Mr. Mina -- I think this is best posed to you and let me know if I'm wrong about that -- a 2023 GAO report titled Facial Recognition Services, Federal Law Enforcement Agencies Should Take Action to Implement Training and Policies for Civil Liberties indicated that CBP had not assessed whether staff had appropriate skills and competencies to use facial recognition services. Can you explain whether this is still an accurate conclusion?

MR. MINA: I think I've actually -- Ms. Sabatino just raised it in her testimony about the training that's being developed for April 2024.

COMMISSIONER JONES: All right, okay. So the training has not yet gone into effect?

MS. SABATINO: The training has been under development and we expect implementation in April 2024. I will say I think it's specifically training for facial recognition technology, but a lot of the elements of that are covered in the overarching training that we do today. But we are consolidating

that and working with our Office of Training and Development specific to that specific technology.

COMMISSIONER JONES: And relatedly, is it your sense that the people who are running these facial -- these FRT searches, I'll describe them as, that they are aware of this sort of generalized 2019 guidance that Mr. Mina mentioned regarding the use of biometric data in the First Amendment context?

MS. SABATINO: We do quite a bit of outreach with our teams with respect to a variety of the different challenges that have been raised to us in terms of our application of our authorities and the regulations that we uphold. So I think in refining this specific training for April 2024, I think it will enhance our ability to target our frontline officers.

COMMISSIONER JONES: Okay.

COMMISSIONER GILCHRIST: Madam Chair?

CHAIR GARZA: Commissioner Gilchrist.

COMMISSIONER GILCHRIST: So each of you have described in your testimony today internal recommendations and guidance that you have. Would any of you want to share if you think any guidances or recommendations that could work as good policy recommendations for our country?

MR. MINA: I would just say I think

without sort of framing legislation for the country, I think that the facial recognition directive is a great model for how the Department or government agencies think about, you know, how to use the technology. Again, I think that, you know, as we've all kind of highlighted, you know, one of the important parts of this is both forward and backward looking, you know, looking at our existing uses as well as thinking about how do we build this out going forward. You know, I think that, you know, one of the things that my office is really keen on is, you know, you heard me say early and often so like, you know, for example, I'm at CBP or I'm at TSA and I think hey, I have this new technology I want to develop or I want to utilize some commercially available technology and that, you know, obviously touches on other parts of the Department as well, but how do I do that? How do I go about doing that? I think there might be civil rights or civil liberties implications.

COMMISSIONER GILCHRIST: Sure.

MR. MINA: And that's where we get involved. And then throughout that, that life cycle of that particular technology or program or policy, we're involved every step of the way. And I think that's really the model not just at DHS but I think

sort of around -- you know, other places, too.

COMMISSIONER GILCHRIST: Anybody else want to go in on that?

MS. SABATINO: And I do think, as Mr. Lim outlined, we have a very unique business use case from what traditionally other law enforcement partners; right? We're not going out and looking for individuals. We are encountering very legitimate travel through ports of entry. But I think certainly in the framework and as I mentioned, we do a lot of work with organizations as well as federal partners to share best practices. I think the partnership we have just within DHS and TSA and sharing, you know, the technology that we use, the testing results that we have, and I think a phenomenal platform through S&T in DHS to help, you know, share those best practices.

But also I think our lessons learned are important to share with our colleagues, not just our best practices; what have we learned through this process and how have we improved because of challenges that we've identified.

CHAIR GARZA: I have a -- do you have --

COMMISSIONER GILCHRIST: No. That's good.

CHAIR GARZA: Okay. I just have a follow-up question regarding privacy and who keeps the data

that is being collected, because I know you mentioned that for non-citizens, it goes and it's stored for, what did you say, 75 years? And then also for citizens, it gets stored for 72 hours I think is what you said? Twenty-four?

MS. SABATINO: It's less than 12 hours, and often --

CHAIR GARZA: Less than 12, okay.

MS. SABATINO: -- deleted pretty quickly.

CHAIR GARZA: I'll correct that. Less than 12 hours for U.S. citizens and 75 years for non-citizens. So who keeps that data?

MS. SABATINO: That is actually sorted to DHS system, IDENT. Please don't ask me what the acronym actually stands for.

CHAIR GARZA: Okay.

MS. SABATINO: It's been around a while. But, you know, a lot of policy and system of record notices that support the retention of that data. I do know it's something that has been evaluated for the timeframes that the data is currently held. It is, you know, certainly a tool that we use to identify photos for individuals who have previous DHS encounters that we used to help build galleries at times for the TVS system.

CHAIR GARZA: Yes. That was going to be my follow-up question is, what is it ultimately used for, that database?

MS. SABATINO: I would defer to DHS. I don't know that Peter is the right person or if we have someone to speak to the totality of the IDENT system.

MR. MINA: I think we can take that as a get back, Madam Chairperson.

CHAIR GARZA: Okay. Thank you. Commissioner Jones?

COMMISSIONER JONES: Yes. Would one of the panelists please identify whether DHS has a process or issues guidance for how FRT funding grant recipients, including sub-recipients, contractors, subcontractors are responsible for complying with the Civil Rights Act of 1964, specifically Title VI?

MR. MINA: So first of all, just as it relates to Title VI enforcement generally, that is the responsibility of my office. We have a whole group that actually does look at Title VI enforcement, and we work with our partners, a lot of grant-making is obviously through the Federal Emergency Management Agency.

COMMISSIONER JONES: Yes.

MR. MINA: And so we work really closely with our colleagues in FEMA to make sure that we are enforcing the requirements of Title VI. And then I think I would say again, I think we can also take some of the specifics about facial recognition as a get back. But I think that there is across the board -- like there's no special delineation based on one use case versus another. I think our goal really is to make sure that we are ensuring that Title VI is enforced in a meaningful way for DHS grantees and recipients of federal financial assistance.

COMMISSIONER JONES: So there's no -- your testimony is that there is nothing specific to facial recognition technology in particular and --

MR. MINA: There's not a -- like I think if I'm understanding your questioner, Commissioner, like there's not a special policy as it relates to Title VI enforcement --

COMMISSIONER JONES: Right.

MR. MINA: -- and facial recognition. No, there isn't. I think it's just a matter of our -- at least at this point, it's a matter of our general enforcement of the statute.

COMMISSIONER JONES: Yes. But doesn't it seem to you that there ought to be a specific policy

for FRT?

MR. MINA: So again, I think that's probably a broader conversation in the Department, but I think what I would say to that is that I think that there are, in any of our interactions with our federal grantees or federal -- recipients of federal financial assistance -- excuse me -- I think it's important for us to stress the importance of Title VI enforcement, adherence, and that's really the responsibility of our office and as a department. And so I think that yes, I hear you and I respect the idea that facial recognition is a part of that picture. I just don't know that it's a picture unto itself, if that makes sense.

COMMISSIONER JONES: I hear your testimony.

CHAIR GARZA: I'm going to turn to the Commissioners on the phone, if there are any questions?

VICE CHAIR NOURSE: No questions.

CHAIR GARZA: Okay. Just -- I have one last thought, one question here. Is there an effort to coordinate, you know, policies and procedures and training and practices across all of DHS, or is everyone talking to each other?

MR. MINA: I think the answer to that is yes, Chairwoman, I think that we are.

CHAIR GARZA: Okay.

MR. MINA: I think that the Directive is certainly a launching pad for that but yes, I think that -- I mean again, you know, as the Department's Office of Civil Rights and Civil Liberties, that's our responsibility. And I think that we are -- you know, as the Secretary said, we're a Department of partnerships. And so I think that that really is how we work as a Department is to really, you know, reach across and say, all right.

But again, I think to pick up on -- and I think this might be what you might be -- what like you might say -- is, you know, it is -- it does -- some of the training and some of the guidance is going to be use case specific, and so I just want to be mindful of that as we sort of think about what the enterprise looks like. But yes, I think that, you know, we are talking to one another. And again, even with a Department this large and this diverse, we're making sure that whether that's through the Directive or through our own sort of advice and, of course, mechanisms, that we are sort of cutting across in the way that you're describing.

CHAIR GARZA: Yes, because -- go ahead.

MS. SABATINO: I just wanted to acknowledge that we do have a Biometric Steering Committee Meeting that consists of countless individuals across the Department. I think the last attendee list was about 128 different individuals that participated from different offices across the DHS. But we also have a smaller group with the Office of Biometric Identity Management TSA, CIS, and CBP as well as the CIO's office, the management office that has an executive steering committee as well and the smaller group where we do discuss the operationalization, and facial has been a very big part of that though. It's not the only modality that we talk about.

CHAIR GARZA: Yes. I appreciate that. I mean for me, it's just like you have American citizens interacting with these agencies on a regular basis, right? When you're flying into the country or you're entering a port of entry, we're interacting with OFO. You know, we're interacting with TSA. I don't think the vast majority of American's are aware that they can opt out. I opt out but it's always a gamble. I don't know how -- what reaction I'm going to get, but I think that having uniformity and information at TSA

and OFO, you can opt out. It's not an issue. It's not going to cause you any problems. You know, I think that's just like a small thing, right, but I appreciate what you all are trying to do.

And I think uniformity where you can have uniformity is really critical, because I do think these technologies can lead to safer communities, but we just have to make sure that we're balancing it with civil liberties and civil rights protections.

So Commissioner Jones, would you like --

COMMISSIONER JONES: Yes.

CHAIR GARZA: -- to be recognized?

COMMISSIONER JONES: I would. I've got two additional questions --

CHAIR GARZA: Okay.

COMMISSIONER JONES: -- while we still have a little bit of time. The first is -- and again, this is for anyone to answer on the panel -- are DHS facial recognition grant-funding recipients required to conduct periodic, ideally independent, audits of the use and accuracy of their facial recognition technology programs?

MR. MINA: So I want to do a little bit of homework on that, Commissioner Jones, if that's okay. I think that, you know, while there are certainly, as

I mentioned in the Directive, like certain requirements that apply sort of across the board, your federal, state, local, territorial, you know, again, people who interface with the Department. I wanted to make sure I answer your question accurately and completely.

COMMISSIONER JONES: And just as a follow-up to that --

MR. MINA: Yes.

COMMISSIONER JONES: -- question, and I appreciate your getting back to us on that, I mean DHS does have the authority to implement some kind of rule saying that if you are going to receive our funding for purposes of using facial recognition technology, these are the expectations that we have of you, isn't that correct?

MR. MINA: I think with any grant, like as you say, there's certainly, you know, expectations that we can set for the grantee.

COMMISSIONER JONES: And then Madam Chair, if you don't mind, my other question is can someone describe the process of sharing facial recognition technology with state and local partners and what that looks like, cause we know that FRT, at least in the law enforcement context, is, just given the nature of

federal is and the way our criminal justice is, mostly done at the state and local level.

MR. MINA: So again, I think that -- and, you know, open up to my colleagues here -- I think that varies based on the use case, and so a lot of the use cases that you've heard about today are pretty DHS specific. So, you know, I don't know -- like for example, I don't think that there is necessarily broad sharing of that technology, you know, sort of outside the proverbial four walls of the Department. I think I'm answering -- if I'm understanding your question correctly.

COMMISSIONER JONES: I imagine like the NYPD, for example, which has its own counterterrorism --

MR. MINA: Yes.

COMMISSIONER JONES: -- is working with DHS on some of this stuff.

MR. MINA: Again, I think there's probably broad -- and I'll use this term generally -- I think there's broader information sharing certainly, but I want to be careful about, you know, misstating whether or not there's actual hey, we're using technology x algorithm y, you should use it too, if that makes sense.

CHAIR GARZA: Okay. Well, I want to thank all of the panelists for your testimony cause I -- if there are no more questions at this point. I appreciate your testimony, answering our questions, and look forward to hearing back from you all on some of the questions that we asked here today.

I would like for you all to go over to the sign after we close up so I can take a photo. We really do appreciate you being here.

So we're going to go ahead and break for one hour for lunch and reconvene promptly at 1:50 p.m. for our next panel.

(Whereupon, the above-entitled matter went off the record at 12:42 p.m. and resumed at 2:00 p.m.)

CHAIR GARZA: Welcome back, everyone, and thank you for your continued attention to this important topic. As I have indicated to our previous panel, each panelist will have seven minutes to speak. Following the conclusion of the panel presentation, commissioners will have the opportunity to ask questions within the allotted period of time. And I'll recognize commissioners who wish to speak.

I will strictly enforce the time allotments given to each panelist to present his or her statement and unless we did not receive your

testimony until today, you may assume that we read it. So please use your time to summarize your testimony in the seven minutes that you have allotted for you.

Panelists, please notice the system of warning lights that has been set up. When the light turns from green to yellow, that means two minutes remain. When the light turns red, panelists should conclude your statements, so you do not risk me cutting you off mid-sentence. My fellow commissioners and I will do our part and keep our questions and comments concise.

So now we're going to proceed with our third panel which will address guidance for meaning federal oversight. In the order in which they will speak our panelists are Nicole Turner Lee, Ph.D., Senior Fellow, Governance Studies and Director, Center for Technology Innovation at the Brookings Institution, welcome; Patrick Grother, scientist, National Institute of Standards and Technology; Laura MacCleery, Senior Director of Policy at UnidosUS; Deidre Mulligan, Principal Deputy U.S. Chief Technology Officer, White House Office of Science and Technology Policy. Welcome. Thank you for being here.

I'm going to ask each of you to raise your

right to be sworn in. Will you swear and affirm that the information that you are about to provide us is true and accurate to the best of your knowledge and beliefs?

Affirmative from all of the panelists. We'll go ahead and begin with Dr. Turner Lee.

DR. TURNER LEE: Thank you, Chairwoman and distinguished members of the Commission for this invitation to testify on this important issue on the federal use of facial recognition technology, and I'll abbreviate it throughout my testimony as FRT. The Brookings Institution is an evidence-based, nonpartisan research think tank and my own experience intersects race, technology, and social justice and the policies that support equitable AI.

I spent the last few months as a member of the National Academies Appointed Research Committee on the use of facial recognition which was sponsored by the Department of Homeland Security and the FBI. The committee's final report was published in January 2024, and offers a series of technical explanations, challenges, and recommendations in response to the increasing use of FRT by law enforcement. Concerns around equity, privacy, and the protection of existing civil rights emerge as critical themes of the report,

as well as the need to think about future use cases by federal agencies and other police entities, including Customs and Border Patrol.

In my testimony today, I just want to reinforce the report's recommendations, particularly those that support reasonable and equitable standards when it comes to FRT use and make specific calls to federal legislators, in particular, to formalize guard-rails for law enforcement and other federal agencies using the technology.

In addition, when individuals and their families are harmed, we have an obligation to provide some sort of remuneration or appeal to those affected individuals especially if the Government is at fault. In my written statements, I go into more detail on what those would look like. In my oral statements, I'll be brief.

I think that you've already learned from the previous panel about the technical inadequacies, as well as opportunities that FRT presents. The key takeaway is that particular features are not commonly training models, such as darker skin hues, they do not optimize for performance with regards to those characteristics. NIST facial recognition vendor test has found that algorithms used by law enforcement

perform worse on faces of women and people of color and there's no mere abstract technical concern here. To date, six people are known to have been falsely arrested due to incorrect FRT matches, all of whom are Black, which is continuing our history discrimination and over surveillance of people of color.

I want to walk you through the case of Porcha Woodruff from Detroit, the woman wrongfully arrested due to FRT. One morning, earlier this year, she was getting her two children ready for school when suddenly six police officers were on her doorstep with an arrest warrant for carjacking and robbery. Being eight months pregnant, she was arrested and taken to a detention center where she remained there for hours. Exhausted upon release, she was taken to the ER where she was found to have low blood pressure due to dehydration and contractions due to stress. Her arrest was based on an outdated photo processed by Detroit police which identified her as a match, despite the suspect in the grainy photo clearly not being pregnant. She is now suing the City of Detroit after spending time at the station and money to prove her innocence and this does not include the cost and the greater trauma of her children who witnessed their mother's arrest.

Experiences like Woodruff's are not only due to faulty technology, but inadequate procedures used by the people applying it, as well as possibly racially-motivated policing. Although there is not much public information on the internal procedures that police officers use when they are deploying the technology, these six cases have some things in common. They do not require a supervisor's signoff on the match. They used non-eye witnesses to identify the suspect from a lineup, and they proceeded with an arrest without any corroborating evidence.

Police departments clearly need internal guidelines and requirements around the development, testing, and use of the system, to encourage responsible, equitable, civil rights-preserving outcomes which goes to my recommendations.

First and foremost, we need to make sure that the government leads by example by being responsible and ethical in our use, not just in law enforcement, but among other government agencies that actually deploy it. We gave a lot of great recommendations that I will not repeat for the interest of time in the National Academies report and I urge the Commission to take a look.

Further, we need increased appropriations

to the National Academies and the National Science Foundation to do more research when we're trying to think about more inclusive data sets that allow these matches to be made and to think about problems that may not necessarily be only couched about civil rights that have sociological and technical implications.

The Federal Government has to obviously come to agreement on what kind of congressional guidance we want. We've been sitting here on issues of data privacy and others and without any type of congressional support those guardrails will still be unaccountable. But most importantly, I think is we're having this conversation on federal mandates. We have to keep in mind that the Federal Government only has oversight in the area of policing over federal police. It is where states have more jurisdiction in the use of these technologies and they often go under the radar with the same type of opacity when it comes to training certification on use.

With that being said, one recommendation is to come up with a federal fair and equitable use standard, one that could be co-developed between federal and state police, but includes requirements for robust public disclosures and something I didn't get a chance to mention in my statement, my written

statement, but I'll say it now, potentially citizen engagement. Being able to have that national fair and equitable use standard allows us to give some guidance, as well as some enforcement, to law enforcement, in particular, if they use it.

And I should suggest that the same type of standards need to apply to federal agencies. In my written statement, I talk about other use cases like the IRS where we're seeing potentially with students who have facial recognition embedded into the back ends of computers or school-issued laptops. We're seeing examples in healthcare. These future use cases are going to have implications particularly for people like Porcha Woodruff, who had no agency or no awareness or how these technologies were going to be used.

And my final recommendation is what do you do with Ms. Woodruff, who now has to pay the legal expenses for her innocence and also deal with the trauma of her children?

One of the considerations that we touched upon lightly in the National Academies report, but I'll stress it here in my closing statement is that the Federal Government should consider the possibility of retribution and compensation. Those individuals

were already disadvantaged before the start, and now they have to find the legal fees to expunge their records because now they're actually in the system.

What we do to actually remediate the harms of people like Ms. Woodruff from algorithmic discrimination is particularly important. And who pays the costs? Well, often times, it's the individual when really, if the government makes a mistake, we need to figure out how to make it right.

In sum, these recommendations before all of you, acting on the proposed recommendations of the National Academies report or at least considering them, developing a research agenda that allows us to look at the sociological and technical implications and maybe do something different by finding more inclusive data sets, developing that reasonable and equitable standard for FRT use among Congress or other federal agencies that are now going to be responsible for responsible and ethical use, and then finding ways to help people like Ms. Woodruff, so that they don't walk away from these scenarios even worse scarred than how they started.

Thank you very much and I look forward to your questions.

CHAIR GARZA: Thank you so much, Dr.

Turner.

And we're going to now hear from Mr. Grother.

MR. GROTHER: Thank you, Chairwoman Garza, and members of the Commission. I am Patrick Grother, scientist in the Information Technology Lab, part of the Department of Commerce, National Institute of Standards and Technology, NIST. Thank you for the opportunity to appear to discuss NIST's role in standards and testing for facial recognition technology.

NIST's role in biometric and facial recognition technology is to respond to Government and market requirements for biometric standards, including facial recognition technologies by collaborating with other federal agencies, law enforcement, industry, academic partners to conduct research, measurement evaluation, and interoperability to develop metrics to support timely development of scientifically valid, fit-for-purpose standards, and to develop the required conformance testing architectures and testing tools.

NIST's work improves the accuracy, usability, and interoperability and consistency of identity management systems and ensures that the United States' interests are represented in the

international arena. NIST's research has provided state of the art technology benchmarks and guidance to industry and to U.S. Government agencies that depend upon biometric recognition technologies.

Accuracy of face recognition today is assessed by measuring two types of error that the software can make, false positives and false negatives. A false positive means that the software wrongly considered photos of two different individuals to be the same person. A false negative means that the software failed to match two photos of the same person. This is important and has different consequences for different applications.

A bit of background, for two decades, NIST's biometric evaluations have measured the core algorithmic capability of recognition technologies and reported the accuracy throughput reliability and sensitivity of algorithms to data characteristics. For example, noise or compression as a subject characteristic, for example, age or gender. NIST biometric evaluations advance the technology by identifying and reporting gaps and limitations of current biometric recognition technologies. NIST evaluations advance measurement science by providing a scientific basis for what to measure and how to

measure. NIST evaluations also facilitate development of consensus-based standards by providing quantitative data for development of scientifically sound standards.

Since 2000, NIST's face recognition vendor tests have assessed capabilities of FRT for one to many search applications and one-to-one verification. In 2023, the program was split into two parts, facial recognition technology evaluation dealing with who is in the photograph, and the face analysis technology evaluation addressing things about the photograph such as its quality. These parallel programs are today known as freight and fate. Participation is open to any organization or otherwise and there is no charge for participation. And being an on-going activity, participants may subject their algorithms on a continuous basis. The algorithms are submitted to NIST by corporate R&D labs and universities. They are prototypes and are not necessarily available as mature products.

We post results on our website and identify the developer of the algorithm alongside. We do not do training of recognition algorithms. The evaluations provide the U.S. Government with information to assist in determining when and how

facial recognition technology can be best deployed, how our results help identify future research directions for the FR community. NIST provides technical guidance and scientific support for analysis and recommendations for utilization of face recognition technologies to various U.S. Government and law enforcement agencies.

Measurement of demographic effects. While face recognition accuracy has been supported by adoption of portrait photography standards, first developed by NIST in the late 1990s, false negatives still occur with photos of significantly degraded image quality and with change of appearance such as due to injury or natural aging.

In December 2019, NIST released Interagency Report 8280 which quantified the effect of age, race, and sex on face recognition performance. The report analyzed one-to-one verification and one to many search algorithms separately and found that demographic differences in false positive rates are often much larger than for false negative rates. The report emphasized that the two types of error have different impacts and that these depend heavily on the application of the technology. The report recommended operational testing that end users should know your

algorithm when fielded with their populations in their applications.

The analyses in the 2019 report are now applied to all algorithms submitted to our benchmarks. False negative rates remain generally low such that demographic variations are small. False positive rates remain variable and highly algorithm specific with higher rates observed in women, in the elderly, and the young compared to middle-age adults.

Regarding race, we see higher false positive rates in Asian and African faces, relative to those of Caucasians. These effects apply to most algorithms, including those developed in Europe and the United States. However, a notable exception is that some algorithms developed in Asian countries give lower false positive rates with Asian faces than they do with Caucasian faces.

While the NIST studies have not explored the relationship between cause and effect, the AI literature documents many instances where imbalanced training data causes under performance with underrepresented groups.

In 2022, we published NIST Interagency Report 8429 which was developed with Homeland S&T and with industry to establish summary measures for

stating overall magnitude of demographic effects. This work was used to guide the development of an ISO standard which puts requirements on tests. In 2024, we will publish a report which applies to standard demographic summaries to recent one to many search algorithms.

Additional recent work shows that measurements of performance across demographic groups is warranted in applications beyond just recognition. NIST Interagency Report 8491 looked at the performance of algorithms tasked with detecting whether a photograph is an attack photograph, meaning somebody wearing a face mask or presenting somebody else's photo. In addition, age estimation algorithms are also subject to demographic effects, nothing to do with recognition.

In conclusion, NIST is proud of the positive impact we have had in the last 60 years on the evolution on biometric capabilities. With our extensive experience and broad expertise both in its laboratories and in successful collaborations with private sector and government agencies, NIST is actively pursuing the standards and measurement research necessary to deploy interoperable, secure, reliable, and usable identity management systems.

Thank you for the opportunity to testify today.

CHAIR GARZA: Thank you, Mr. Grother. We'll now hear from Ms. MacCleery. Please proceed.

MS. MACCLEERY: I am Laura MacCleery, Senior Policy Director. I am so grateful to the Commission for the opportunity to testify today on behalf of UnidosUS, a nonprofit, nonpartisan organization that is the largest Hispanic civil rights and advocacy organization.

There is a clear and urgent need for updated laws and regulations to address ongoing imprisonment by uses of FRT and other technologies and to apply constitutional principles like due process, equal protection, and privacy. How the Government sets standards for technology acquisition by the Federal Government including by law enforcement and immigration agencies could be a substantial lever to drive more responsible and democratic process and design.

Because communities of color and immigrants are the first to be targeted and the last to benefit from technological change, this is one of the most important civil rights issues of our time. To date, we simply have failed to align constitutional

rights with the chief and routine surveillance of movement and biometrics aided by data collection on every aspect of our lives.

And I wanted to depart from my remarks to reflect on some things that happened this morning. Although we heard from Clearview that they use public information, I want to flag that side steps the question of consent and our expectations about the use of our personal data. Clearview acknowledged, for example, that there were expectations of privacy and the need for consent by its customers, but didn't say what it thought about consent for the rest of us who merely use the internet and didn't likely have an expectation that our information would be scraped, compiled, and used to train AI models and facial recognition technology. This is a conversation in some ways that circles around the issue of consent.

And the same theme came up in the discussion around the airport. 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 as well informed as you, Chairwoman Garza, 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? That is the question that I think we have to grapple with when we're designing systems that can counter balance our need to preserve civil liberties and protections for our constitutional safeguards against the exigency that we have around the exercise of police power or immigration enforcement. I think we don't side step that by a mere technical discussion of standards. 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.

So relatedly, I want to make three points today. First, that the current uses of facial recognition technology undermine democratic norms and principles and threatens immigrant communities and communities of color. Second, that rather than providing exemptions or waivers for immigration enforcement uses as was suggested by the Office of Management and Budget's draft AI memorandum, we need enforceable and binding standards for all surveillance technologies and AI models used to scale them.

The question of how to balance state power

with the preservation of appropriate zones for the privacy of individuals and groups within a democracy isn't new. It goes back to our founding and the creation of things like the First Amendment and the Fourth Amendment. Any healthy democracy has to have effective ways to address threats to law and order and the rule of law at the same time that it preserves the space for nonviolent protests, free speech, the ability to travel, and a zone of privacy around the individual that is both intellectual and physical.

Third, our failure to align these systems with any appropriate governance framework perpetuates communities' exposure to unaccountable, opaque uses of technologies including biometric surveillance. We have to formalize ways to elevate the voices of impacted communities in setting policy and set baselines for privacy with better laws that drive more constitutional systems and design.

So many rightly raise the issue of inaccuracies and we've heard a little bit about that today that specifically impact communities of color. We share these concerns. We saw this problem in our work in Puerto Rico on the expanded child tax credit when the Government's IRS ID systems routinely failed to recognize darker skin images of tax filers.

Machine-learning models generally are highly prone to bias inferences and discriminatory outcomes are pervasive. But even if these profound issues of bias could be addressed, there are other fundamental problems to solve as well. So we mainly speak to those here.

For the 62.1 million Latinos living in this country, the risk of over reach from intrusive surveillance are pervasive. Perceived efficiencies from current and planned uses in criminal justice, immigration enforcement, and related use cases, will likely lead agencies to continue to gloss over deeply concerning data security, stewardship, privacy, and civil liberty concerns. And I think we heard about some of those gaps this morning in terms of the training, gaps that were flagged by GAO that still haven't really been acted on. There's some kind of module in progress, so we don't know what it is. An interim memo or an interim policy that hasn't seen the light of day, there's lots more work to do around transparency and accountability at the basics.

It is important for this administration to act decisively to address these risks. Immigrant and mixed-status communities are canaries in the coal mines on civil liberties because they are positioned

as test cases for policies that roll back all of our shared liberties. Rather than exemptions or waivers for law and immigration enforcement uses, we need enforceable and binding standards.

In my testimony, I explain how the NIST AI risk management framework provides these seven factors that should be applied to any use of AI including around FRT. We also face a rising risk of so-called automation bias which is a propensity to place undue faith in outputs from automated tools. These concerns are heightened when power imbalances are pervasive and there is every incentive given a need for urgent situational judgment such as the current policing or at our borders to disregard the tool's limitations.

Although the NIST framework calls for AI to be privacy enhancing, the memo's waivers would allow the most problematic and race-infringing use cases of AI to continue. We will not get to a consensus on how we can regulate privacy, unless we grapple very specifically with the hard use cases, otherwise, we're just circling around the drain.

Our failure to align these systems with any appropriate governance framework often means that communities are subject to models that are unaccountable and opaque. We call in our testimony

for a multi-faceted governance model that includes inclusive Red Teaming, impact assessments, consumer complaint collection, a public leaderboard for metrics, and a requirement for consumer advisory committees for each agency, sub-agency or department. They have to be able to tell technologists what they may not know, they do not know, about the way technologies show up in the world and with their lived experience.

Setting a national floor on privacy also remains a high priority and is essential for establishing key safeguards for all of these technologies. We deeply appreciate your interest in this process and we stand ready to assist the Commission.

CHAIR GARZA: Thank you, Ms. MacCleery. We're going to now hear from Professor Mulligan.

MS. MULLIGAN: Chairwoman Garza and distinguished members of the Commission, thank you so much for the opportunity to testify today about the U.S. Government's use of facial recognition technology. I want to start by thanking you all for the attention you're paying to this issue and the work that goes into holding an event like this to hear from all stakeholders.

I'm Deidre Mulligan. I currently have the privilege of stepping away from my job as a professor at Berkeley to serve as a principal Deputy Chief Technology Officer in the White House Office of Science and Technology Policy. OSTP, as we are commonly known, is an interdisciplinary team working to maximize the benefits of science and technology to advance health, prosperity, security, environmental quality, and justice for all Americans. We carry out this mission by advising the President and senior advisors in the administration on key issues related to science and technology and by coordinating Federal Government technology policy and priorities.

I want to start with one clear message. The Biden-Harris administration recognizes the risks of facial recognition technology and we are taking bold action to address them. When this technology doesn't work or when it's used irresponsibly, we've seen invasions of people's privacy, violations of fundamental First Amendment freedom, and false matches, and wrongful arrests, all of which disproportionately harms people of color. This is unacceptable and unjust. If we use this technology, we must use it responsibly. It needs to work. It needs to protect people's rights. It needs to protect

their freedoms. It needs to advance equity and most importantly, it has to adhere to our fundamental obligation to ensure fair and impartial justice for all.

Advances in technology have challenged us before, right? Each leap in capability brings new opportunities and with them new risks. I want to say to you today that deciding how and when to use and refuse technologies including facial recognition technology is a key way our nation manifests our values. That is why before AI chatbots and image generators were all the news, the White House released the Blueprint for an AI Bill of Rights. It clearly states our values in a time of rapid technological change. It says we must protect the American public in the age of artificial intelligence. Steering by the light of those values last year, President Biden signed an Executive Order on the safe, secure, and trustworthy development and use of artificial intelligence. And now the administration is finalizing guidance that will include requirements of the U.S. Government's use of AI including facial recognition technology.

These actions are in a context. This administration's commitment to equity and using

technology to support the public interest to ensuring protections for our safety, security, democratic values, and civil rights pervades everything the administration has done.

Dr. Turner Lee talked about the importance of data. On his first day in office, the President signed an Executive Order establishing a working group of equitable data, right, focusing on making sure that the data we use to make decisions across all of government is representative and robust and meets the needs to advance equity.

We've heard quite a bit about state, territorial, local, and Tribal use of facial recognition technology. Part of the President's Executive Order to advance effective accountable policing directed the Department of Justice, the Department of Homeland Security, and the Office of Science and Technology Policy, specifically my team, to identify privacy, civil rights, and civil liberties concerns and recommend best practices to the use of technology including FRT. Part of this effort, we will be issuing a report that includes recommended guidelines for federal, as well as state, Tribal, local, and territorial law enforcement agencies and technology vendors.

You've already heard from Dr. Lee, Dr. Turner Lee, about the National Academy of Science's study that's supporting this work.

I want to turn specifically to the Office of Management and Budget guidance for how federal agencies can use AI responsibly. This is an exceedingly important effort. The OMB draft guidance released for public comment last year would establish a rigorous set of risk management processes and requirements for government use of rights impacting AI including FRT. This includes impact assessments to document the intended purposes, benefits and risks; testing requirements, not just in the lab, but in the field, right? We need to actually view these things as socio-technical systems and we need to understand their real-world effects. On-going monitoring and thresholds for periodic human reviews; requirements for agencies to identify, assess, and mitigate algorithmic discrimination; responsibility to notify individuals, particularly when AI negatively affects their rights and to provide them with the opportunities and the material they need to challenge adverse decisions; and importantly, as we heard from Ms. MacCleery and Dr. Turner Lee, requirements to consult and incorporate feedback from affected

communities. This guidance would be the most prominent, national policy anywhere in the world to affirmatively center civil rights in the design and use of technology by government.

Now even with this guidance, we know there is still important work to be done. OMB has requested public input on how privacy impact assessments may be more effective at mitigating privacy risks, including those that may be exacerbated by AI and other advances in technology. We encourage all stakeholders to submit input to inform how privacy impact assessment can best ensure privacy protection for government use of FRT and other technologies.

In addition, OMB is tasked with identifying and evaluating agency practices for procuring commercially-available information and considering standards for its collection, processing, maintenance, and use. Such information is of critical importance because we know it is often the fodder that is used to develop FRT and other technologies.

In closing, I want to emphasize that there has simply never been a more critical time to ensure technology works for every member of the public and protects our rights and our values, as well as our safety and security.

I want to recognize the efforts of this Commission and the important work you're doing to ensure the Federal Government is protecting our civil rights and I look forward to working with you to make progress on these critical challenges and opportunities. Thank you so much.

CHAIR GARZA: Thank you so much, Professor Mulligan. At this point, I'm going to open it up to the Commissioners to ask any questions of our panelists. Commissioner Jones?

COMMISSIONER JONES: Thank you, Madam Chair. I have a question for Mr. Grother. We heard earlier from someone at NYU's Policing Project.

And I want to quote from Ms. Kinsey's written testimony. And I would like for you to respond to it, because it directly talks about NIST.

She writes, the proponents of law enforcement's use of facial recognition often claim that algorithm myth testing conducted by the National Institute of Standard and Technology provides sufficient independent validation of system performance. This is false.

Although NIST testing provides an important benchmark of algorithms' technical capabilities, NIST doesn't test these algorithms on

the actual low-quality images used by law enforcement. What are your thoughts on that statement?

MR. GROTHER: Yeah. It's essentially true. We use data that we've got. I think though that the case in point there is that it's been a decade since we ran a test of surveillance data.

So this is low quality data that you would collect, maybe outdoors. We're about to remedy that situation in 2024 by rerunning that benchmark from a decade ago. That does include low quality data. It's --

COMMISSIONER JONES: Can you give me an example of what you mean by surveillance and data?

MR. GROTHER: All right. So this is a photo taken say in a train station. The UK Government provided us with that data a decade ago.

So you've got cameras, you know, in a train station. Many, many people are walking. And if the application there would be to look for terrorists or other individuals, our benchmark is a first step at evaluating how well that would work.

CHAIR GARZA: I want to bring Dr. Turner Lee into this, just because something stuck out to me in your testimony about how film, original film was developed by Kodak.

And I think it's something that not a lot of people know about. And I would love for you to delve into that and kind of how it interacts with what we just heard from Mr. Grother.

DR. TURNER LEE: Thank you for that Chairwoman. So in my testimony as a sociologist, and I was coming before this Commission, I indulged myself in some storytelling and history telling about the history of photography.

Like with other technologies, we see a base model or a base figure for the image. Right? In this case, in photography, it was a white woman whose attributes were so seen as the standard for how we pixelate data.

Now, this was back in, you know, the early '30s when this was happening. Many of you, including myself, remember a Kodak camera and things like that, that had a certain type of pixelation with it.

What the challenge is, when we see these types of AI technologies sort of measured and trained on data that is reference data, that includes a couple of things. Who is in the room when the design and development of these products, right?

And in this case, it was Shirly, the Shirly Card as they called it. And from that

reference, how do we then take that technology and build it out and then bring it for public consumption?

What we've seen in AI, FRT, and many technologies, is that reference gets embedded and baked in as an automatic bias and how we actually train these models.

We're not talking about the research data that comes from people like myself, who are subjected to the IRB and human subjects handling and think about the deviances that come with information. We're talking about market-based data.

So just in the case of the invention of photography, where that pixelation was very much placed on an image reference, it doesn't look anything like me. What happens is, as it becomes more embedded into AI technology, it becomes the base reference.

And so, as Patrick has referenced, and we've been able to see a lot of that data, when it has some of these inaccuracies, much of it has to do with the representation of who's in the database. And the photo capture that was previously mentioned by the Commissioner, also has to do with who is over-represented in certain databases.

So who you find in that reference will automatically, may not be trained on me, but you're

going to find me, because the people who are subjected to over-arrest and deportation, et cetera, were in those databases.

So for those of you who want a history lesson, read my testimony. Because I actually really think that's an important part that we've missed when we talk about photogenic quality, and we talk about the history of photography. Thank you.

CHAIR GARZA: Commissioner Adams?

COMMISSIONER ADAMS: Thank you. Dr. Turner Lee, it's interesting what you just said. And I haven't heard any witness today, and I don't think I've read it, I might have missed it, talk about the marketplace and solving this problem.

Don't companies that do this have an incentive to sell good data and fix the problem you're talking about? Or does that not exist in this space?

DR. TURNER LEE: Well, you know, you'd think that they should. And thank you for that question, Commissioner.

We hope that these technologies, and just for the sake of fairness, are optimized for people like me. We're in the same market.

I'd like to be able to have my technology work and not have it misidentify me or like that young

woman, be falsely accused or have a false positive.

With that being the case, this paradigm of go fast, fix it fast, you know, break it fast and then go back and fix it later, has really driven the technology marketplace where, as it was mentioned by my fellow colleague here, tech companies can go to public with any available data to train these models.

So it's not necessarily a standard as to what the input is. And as we've just heard from Patrick, it's not necessarily, you know, a guarantee that that data that they're even certifying for government agencies, is going to be right.

So to your point, we hope that companies understand the reputational risk and want to stay off the front page of the newspaper. And they also understand the fact that they are missing out on a whole population of people where the technology could be beneficial, not just for law enforcement, but in other use cases.

CHAIR GARZA: Yes, Ms. MacCleery?

MS. MACCLEERY: I just want to comment on Unmaking AI by Dr. Joy Buolamwini to the Commission. As a first-person narrative of, and a political coming of age story, it is quite moving and wonderful to read, but also one woman's struggle to be literally

seen by the technology and all of the work that had to go into her work at MIT to document gradations in skin tone and create a validation system, and then work to do advocacy with the companies to get them to accept.

And they were all over the place in terms of the different companies being more or less receptive to this kind of input and feedback. Some partnered with her. Others treated her as a critic.

And, you know, I think this issue of representation in these tools is super important to understand. Minorities will always be under-represented compared to majorities. Right?

Because that is the nature of being a minority in terms of data points. And the systems don't think in terms of moral outcomes or about what should be.

They think in terms of what is, and they derive stereotypes from that data set. And so there's always going to be a lot of need to correct for that problem that's intrinsic in some ways to the data.

And you have to bring a lot of intention to that problem solving, which doesn't mean, you know, around images that it couldn't be solved and facial recognition that couldn't be solved. But the way that the data are treated around inferences that the large

language models make in general is very difficult to solve for, because the more you chase the sort of most obvious ways that data classification is happening, the more the machine learning model can make inferences from things that aren't classified at all.

CHAIR GARZA: Thank you for that. We're going to go to Commissioner Magpantay and then Vice Chair Nourse on the phone.

So we'll start with --

COMMISSIONER MAGPANTAY: I have four questions. One for each of them. Sorry you all. It's good. Okay.

So, Mr. Grother, at NIST, so obviously we've heard this cited often and often again. We see higher false positive rates in Asian and African faces relative to those Caucasians, and I get it.

So what do we do? How do we mitigate that? And I heard you say training. Is that algorithmic training? Is that user training? I don't know. And I'll look to you for that question -- for that answer.

MR. GROTHER: Yes. Thank you for the question. And it goes to Commissioner Jones's question as well. Low quality data is not necessary to observe these problems. These problems with

different races, different regions of birth say, exist even with high quality photos.

So this is an algorithm responsibility to fix it. And we've engaged the developers. We've given them a summary metric to optimize.

This is FitBit for race recognition. To give them a single number that they need to minimize and it's essentially the disparity between error rates across demographic groups.

Photography, as Nicole pointed out, is a separate problem that drives false negative rates. It's a smaller problem, but it can exist.

And it's due diligence on the people who arrange for photographs to be taken. So the people who build cameras, people who install lights to fix that problem. I don't know if I answered the question.

COMMISSIONER MAGPANTAY: No, I -- that was excellent. I mean, especially making error rates equal across all demographic groups.

It doesn't solve the problem, but at least it resolves the racial disparity, the racial ethnic disparity. So I do understand that. Excellent. Thank you.

MR. GROTHER: All right.

COMMISSIONER MAGPANTAY: Second question. Ms. Mulligan at the White House. I read your testimony carefully. The Executive Order issued on May 22, where the President directed DHS, DOJ to issue best practices and compliance.

So I think I heard in other testimony, it said that other reports that only three of the seven agencies are actually doing it. So what's going on with implementation and compliance with the President's Executive Order?

MS. MULLIGAN: So the work with DHS, DOJ, and OSTP that was specifically called for under the Accountable Policing EO, is ongoing and underway. It is to produce a report that will provide guidance and best practices.

I believe earlier today you heard from GAO perhaps, the GAO report, which I read in full. And the questions about compliance with existing guidelines, for example, to conduct privacy impact assessments, is something that I, as I understand from GAO's report, both DHS and DOJ have committed to improve.

I think that the OMB draft guidance that I have provided information about will apply across agencies, is rigorous, and goes well beyond the

current requirements that are placed on any agency.

And with those requirements in place, we will be looking not just to improve privacy practices, not just to improve the performance of algorithms in the lab, but to actually address the ways in which these systems affect people all across the country in practice.

And to make sure that they do so in ways that respect people's privacy, advance equity, expect -- protect their rights and are aligned with our ideas about fair and impartial justice.

COMMISSIONER MAGPANTAY: Right. Okay. No, thank you. And maybe -- if we can just, for this sorry, if we can just get that OMB Directive, and also the Presidential Directives. Because I saw a number of references to them, but I don't know what's in them.

MS. MULLIGAN: Absolutely.

COMMISSIONER MAGPANTAY: So that would be -- if you could provide it, that would be very helpful for our reference.

MS. MULLIGAN: I am happy to have our -- my staff will send them over.

COMMISSIONER MAGPANTAY: Thank you. Third question. Unidos, Ms. MacCleery, thank you for your

service and your great work.

All right. Were you here for DHS's testimony?

MS. MACCLEERY: Yes.

COMMISSIONER MAGPANTAY: All right. Reactions? Thoughts? I'm giving you the floor. What did you -- and I hear --

(Simultaneous speaking.)

MS. MACCLEERY: Well --

COMMISSIONER MAGPANTAY: You know, I really do want to hear your thoughts about what you thought about what they said.

MS. MACCLEERY: I think we have work to do, is what I heard. Right? There are a lot of places where it seems as though the privacy protocols around the retention of data are a little bit surprising.

Seventy-five years seems like a very long time horizon to hold data on any population. For example, I don't understand the sort of fit to purpose of that length of time.

I think immigration is in some ways the absolutely hardest case to think about these questions in. And so it's worth thinking about it at length. Right?

Because there you have to hold all sorts of values and the population affected has diminished rights under our Constitution and in some ways are the most vulnerable. So --

(Simultaneous speaking.)

COMMISSIONER JONES: So, and --

MS. MACCLEERY: Go ahead, Commissioner.

COMMISSIONER JONES: And the national security interests are greater.

MS. MACCLEERY: And the national security issues are greater, absolutely. Right. And the sort of -- and currently the environment that we have around these questions is very polarizing, right, and where we see these things around immigration and immigrants being used politically.

So I think there's -- I think we have to be super intentional about this. It very much concerns me that given the GAO's, I think, D grade, I mean, how would you score that on a letter grade in terms of what the Department needs to do?

That there's been, I think, comparatively little response in a timely way to those recommendations. And I think in general, transparency is super important. Understanding the lack of power on the ground in a lot of the use cases is super

important.

What we know from some of the creation of surveillance towers and other kinds of deployment of data gathering tech along the border, is that there are consequences to that. Migrants take more dangerous routes to avoid what they know about the surveillance towers and face more dangerous conditions in terms of crossing the border.

So we need to understand from a live community perspective, and an impact assessment perspective, what the costs are specifically of use cases, and do a better job of making sure that those things are communicated with maximum transparency and with a concern for the rights of whole communities.

COMMISSIONER MAGPANTAY: Sure. No, I heard that. And I think that's right. Here's what I want to do. So we -- it's a matter of public record, we will get you the DHS testimonies.

If I could invite you, can I just give you some more work? I would love a written reaction to those. Because I know they said a lot.

MS. MACCLEERY: Absolutely. For sure.

COMMISSIONER MAGPANTAY: Right. So if you could just give that to us. Because I would like a balanced understanding, particularly because it's DHS

and the work that is being done.

Last question, Ms. Nicole Turner Lee, thank you.

DR. TURNER LEE: Only my mom calls me that.

(Laughter.)

DR. TURNER LEE: I'm in trouble.

COMMISSIONER MAGPANTAY: No, it's good. So I heard what you said. If the government makes a mistake --

DR. TURNER LEE: Mm-hmm.

COMMISSIONER MAGPANTAY: The victim should be compromised -- should be compensated. And again, and we actually have testimony from, upcoming testimony from defense attorneys. I'm not sure if the witness is here, who will be speaking to that.

And you also said make the data available to public defense. If law enforcement is going to do it, make that available for public defenders.

So I'm not a criminal defense attorney or a prosecutor.

DR. TURNER LEE: Mm-hmm.

COMMISSIONER MAGPANTAY: But they're under-resourced. Could you just say a little bit more about how that happens?

Why don't the traditional, like, torts or false imprisonment, you know, I think Congressman Ted Lieu --

DR. TURNER LEE: Yes, he did.

COMMISSIONER MAGPANTAY: Said that in his written testimony that he submitted, he's not appearing here, said that there should be a private right of action.

But you said that someone could only file a lawsuit. So just walk me through, if mistakes will happen.

DR. TURNER LEE: Mm-hmm.

COMMISSIONER MAGPANTAY: Even with the best system. How do we ensure compensation for the victim so that they can get the justice that, you know, after being wronged?

DR. TURNER LEE: Well, I appreciate that question. I think, in fact, if you don't mind, I'll just unpack it in two ways. Right?

So I think that there's still a lot of conversation that needs to happen in the use of facial recognition when it comes to investigation or use as a forensic tool and the extent to which it's used for prosecution. Right?

And for many of us who have been following

this, you know, Coons, many -- Representative Coons, many, many years ago talked about facial warrants and Ted Lieu the same.

I mean, I have read his work. And I think he's pretty spot on as well as with Congresswoman Clarke, around what do we do to make sure people are protected?

With that being the case, we have to come to the conclusion on the extent to which this is evidentiary. Right?

How do you bring this evidentiary information into a courtroom? And to my point, and if you're going to bring it on the part of people who are making the arrest, are you bringing it on the part of the people who are protecting those who may actually be innocent?

Clearly, as my colleague has said here, Ms. MacCleery, that there's this imbalance of power. And in law enforcement it's even more so.

So what does that mean? I mean, private right of action is al -- is pretty much a three-letter dirty word when we start to talk about that with regard to giving people agency over their data.

In this particular case, there is no level of enforcement. You know, Porcha Woodruff, Robert

Williams, and other folks, other people who are probably -- we don't even know about, can't sue an algorithm for any type of malfeasance.

And so since you cannot sue the model, well, where do you go when you're actually in this space where companies have been indemnified from its use, or there's a mistake that cannot be retractable and you now have other reputational damages and risks.

All the people that were arrested in some way or form, spend a lot of time either incarcerated or with a legal defense attorney. Had to come out and remortgage their home to be able to get that.

That kind of goes, I think, not in tandem. But it's another element of this that we often do not disentangle.

There's the technical side of this. And then, there's the consequence. And on the consequence side, the other thing that we have to look at, as to why I'm actually proposing this, part of what we're seeing with facial recognition is its weaponization against communities that are pretty much over-represented in any type of institutional database that's being accessed for criminal offenses.

So we're not talking about, you know, facial recognition in a healthcare scenario. You

know, when the IRS did it, you know, we caught it in time. But it was for eligibility screening.

The case of law enforcement is a little different. Right? We're talking about the fact that people of color are more likely to be arrested, despite not doing the same amount of crime.

We're already talking about a data set that is over-representative of people of color in it. We're talking about people of color in general who could be walking down the street and just be stopped just because they're walking on the wrong side of it.

My point is they're going to be represented in some type of institutional database and therefore will have some type of institutional reaction.

If the government makes a mistake in some way or form, we should try to figure out ways to not indemnify ourselves from that, from that mass surveillance. Let's figure out how to fix it.

The unfortunate thing, we as securers of this technology, is the last that I'll say, we have no agency over the technologies we buy, we license, we purchase, and we distribute.

We sort of assume that once it's in our purview that it's going to work correctly. And we

indemnify the private companies if it doesn't.

So my point is, at some point, whatever this mechanism is, if the government is going to be at the forefront of deploying these technologies, purchasing them, particularly the federal law enforcement side, we have to take some responsibility in their use.

If we're not going to train and certify people on our staff to use it, then we need to figure out ways in which we protect local citizens from being the victim.

CHAIR GARZA: Thank you.

MS. MULLIGAN: May I ask -- may I say one thing?

CHAIR GARZA: Okay.

MS. MULLIGAN: I do want to note, because I skipped over it, I believe in my spoken testimony, that the OMB draft guidance does have recommendations to manage the risk in federal procurement, because this is an incredibly important area.

And we need to make sure that the technologies we're bringing into the government, meets the standards required for government to use them.

COMMISSIONER MAGPANTAY: That's what I wanted. That's it. I did not know that actually.

And especially the amount of procurement, because we're dealing with vendors, makes a lot of sense.

Yeah, so let's.

CHAIR GARZA: Okay. Well, I appreciate that.

COMMISSIONER MAGPANTAY: Thank you. Thank you.

CHAIR GARZA: I wanted to make one note -- okay. One note, Ms. MacCleery, that I really appreciated that you mentioned that book, Unwavering AI.

I do want to note for the record that we did receive testimony from the author, Dr. Joy Buolamwini, I'm so sorry, the founder of the Algorithmic Justice League.

And before we go to you, Commissioner Jones, I do want to acknowledge that we have Vice Chair Nourse on the phone and give her the opportunity to ask a question.

VICE CHAIR NOURSE: Hello, can you hear me?

CHAIR GARZA: Yes.

VICE CHAIR NOURSE: All right. Thank you. I just wanted to thank these panelists for your service. I am a professor and I'm sitting over here

in Georgetown. And I apologize for not being there.

But you really are doing amazing work. And you're doing amazing work by serving in the government as well. It's difficult, as you know. I know, I've done it before. I used to be across from OSTP.

So I also just want to say, because I've been in and out because of technical difficulties that I want to commend Commissioner Jones and his staff for putting this hearing together. It's really his work that has led us here.

And I'm going to turn it back to them, because they are the ones who have been leading this charge. Thank you very much.

CHAIR GARZA: Commissioner Jones?

COMMISSIONER JONES: Thank you, Vice Chair Nourse. Professor Mulligan, did you have an opportunity to observe the testimony, any of the exchanges during the first panel today?

MS. MULLIGAN: I did not. I did read all of the testimony. But I did not have the time this morning to watch.

COMMISSIONER JONES: Okay. It --

MS. MULLIGAN: I am sorry.

COMMISSIONER JONES: It is totally fine.

You're very busy. And I don't expect you to have done that.

You made a representation at the outset of your testimony that the Biden Administration cares very much about many of the civil rights concerns, if not all of the civil rights concerns that have been expressed throughout the course of today's hearing, and is committed to fairness and equity use of FRT across the federal government.

That representation stands in stark contrast to DOJ's refusal and HUD's refusal to not only send representatives to testify today, but to not so much as even submit written testimony, which is extraordinary to me.

And so two things. First, I hope that you will convey the disappointment of this Commission to the White House when you return to the White House and encourage them to at least produce written testimony, which we have not subpoenaed. Though we could.

And also do you have any additional context that might help explain why HUD and DOJ refuse to cooperate with our requests, which were timely made?

MS. MULLIGAN: I do, like you, believe that it is very important for the federal government.

And as we know, as a member of the Biden/Harris Administration, feel it's very important for us to be here to talk to the Commission about this important issue.

I cannot offer any insight on my colleagues at DOJ and HUD. I will certainly make sure that I communicate your concerns back to both my boss but also to my colleagues at DOJ and HUD.

And I do want to say that the guidance that is in draft form, but that we are working very hard to finalize, is going to set a very high bar. And it is not something that can be ignored by any agency.

And so I hope that by taking this sweeping action that addresses not just FRT, but other ways AI is used, we will be helping all agencies meet the expectations of the American public and meet the goals of this Commission.

COMMISSIONER JONES: I appreciate that very much. And I imagine that that guidance will be dynamic.

And so when we release our report, hopefully our recommendations and our findings will be taken into consideration, maybe to the extent that you would update that guidance with some of those

suggestions.

CHAIR GARZA: Okay. Okay. I see no more questions. I do -- I do have one question for Mr. Grother. And it's about the 2019 demographics report.

You noted that system owners should test their systems on operational imagery to know how well or poorly they work and under real-world conditions. How did that go?

MR. GROTHER: We made the recommendation four years ago. We don't keep track of who does what afterwards.

We would hope they would do it. Obviously it gives you -- it's the acid test. Do it in your data, your population, your environment. That would give you data.

I think operational testing and our standards for operational testing is not done enough.

CHAIR GARZA: And what's the value of operational testing?

MR. GROTHER: Insight into your real system on your real population. The reason you need to do that is because you can't just come up with a monolithic statement of how well face recognition works.

It's all data dependent. Data dependent

means photography dependent, environment dependent, population dependent.

So you can't separate. You can -- you can do some good faith efforts to do testing in the lab. But the operation is where the rubber hits the road.

CHAIR GARZA: Yes. And it's different in the real world versus in some of these controlled, more controlled environments.

MR. GROTHER: Usually. If you take immaculate data from an operation and take it into a lab, maybe it's representative.

But as soon as something changes, the lights go down, somebody changes a light bulb, things could change.

CHAIR GARZA: Mm-hmm. Yes, Ms. MacCleery?

MS. MACCLEERY: I would just add, I think there's also the human factors and training and education about the limitations of the data side that you also need to situate the technology in.

I was very interested in what DHS said they were doing in terms of their Maryland Center around those kinds of advancements. That's a major area where we should have lots of expectations for all technology that's deployed of all kinds.

Especially when it's in use by officials with power making decision making. Right? The staff interacts with the technology.

They need to understand how to use it well, to be trained on its implications. And to understand the legal and constitutional context in which it should be used or not used.

CHAIR GARZA: We appreciate that.

MS. MULLIGAN: Yes, if I could emphasize the importance of that real world testing condition. And, again, the OMB guidance, which is still in draft form, but when finalized, says lab testing is insufficient. Right?

And part of it is certainly about the images and how the algorithm performs with different kinds of probe data, different kinds of lighting.

But it also is about addressing the socio-technical system, which is about automation bias. It's potentially about the people who are using the system and how tired they are.

And so monitoring and oversight, so we actually understand its performance in the field, is critical if we really want to achieve our goal.

CHAIR GARZA: And, Dr. Turner Lee?

DR. TURNER LEE: Yes. And if I may add,

so as you all are doing some fact finding, a couple of things I want to put before you as well.

The National AI Research Resource, I believe it is, is really charged with doing some of this responsible technology research, where they actually should be looking at inclusive data sets.

So I would encourage the Commission to look at several entities, including the new AI Safety Institute, to put that on their radar, the ways in which we make inclusive technology use and ways we would make, you know, technical -- we're testing for technical infallibilities.

But the key thing is, we have some of those entities that are actually cross-functional that are bringing together researchers there.

One other thing that I will also note, given the sensitivity of the Brookings Institution in this work as well, we've recently deployed an AI Equity Lab. Which is actually intercepting many of the conversations that we're talking about now.

But really bringing together the people who are technologists, sociologists, philosophers, ethicists. People from diverse backgrounds too really co-evolve what we think are some of the better practices when you are synergizing civil rights

protection, technical cadence, and the ability of the technology to perform in high-risk scenarios.

So things like AI in housing, education, criminal justice, you name it, financial services. We're going beyond the back of the napkin, but really trying to come back to you all with some really good data.

So we're happy to also submit that for comment, because we'll be starting some of that work as well.

CHAIR GARZA: And thank you for that. I want to thank all of you again for coming here today and engaging in this really robust conversation about, you know, not just the emerging technology, but what are the solutions?

How do we create some safeguards and ensure justice is at the heart of this?

So with that, we're going to go ahead and take a ten minute break and reconvene at 3:15. If the panelists wouldn't mind indulging us in a photograph on the other side, we'll see you over there. Okay.

(Whereupon, the above-entitled matter went off the record at 3:03 p.m. and resumed at 3:20 p.m.)

PANEL 4

ACTIONS FOR STRENGTHENING RESPONSIBLE FEDERAL FRT

PRACTICES AND POLICIES

CHAIR GARZA: Good afternoon, we're reconvening at 3:20 p.m. Eastern, and we're going to now proceed with our fourth and final panel, Actions for Strengthening Responsible Federal Facial Recognition Technology Practices and Policies. Thank you to the panelists for being here today.

During the briefing, each panelist will have seven minutes to speak, and after each presentation, after the presentation closed, the commissioners will have an opportunity to ask questions within the allotted time that we have, and I'll recognize commissioners who wish to speak, so please indicate to me that you want to speak. I will strictly enforce the time allotments for each of our panelists, so please summarize your statement as best you can within the seven minutes, and focus your remarks on the topic of our briefing.

Panelists, please notice the system of warning lights that we have set up. When the light turns from green to yellow, that means two minutes remain, when the light turns red, panelists should conclude your statements so you don't risk me cutting you off mid-sentence. I will endeavor not to do that, but my fellow commissioners and I will also do our

part and keep our questions and comments as concise as possible.

So in the order in which our panelists are speaking, we have K.J. Bagchi, Vice President Center for Civil Rights and Technology, from the Leadership Conference on Civil and Human Rights, Brian Finch, partner at Pillsbury Law, Michael Akinwumi, Chief Responsible AI Officer, National Fair Housing Alliance, welcome, Clare Garvie, Fourth Amendment Training and Resource Council, National Association of Criminal Defense Lawyers, and finally Dr. Heather Roff, Associate Fellow, Leverhulme Center for the Future of Intelligence, University of Cambridge, Senior Research Scientist Center for Naval Analysis. Thank you and welcome.

I'm going to ask each of you all to raise your right hand to be sworn in. Will you swear and confirm that the information that you are about to provide us is true and accurate to the best of your knowledge and belief?

All panelists indicated yes. So we're going to go ahead and begin with Mr. Bagchi, if you would indulge us.

MR. BAGCHI: Sure, thank you. Good afternoon, Chair Garza, Vice Chair Nourse, and

distinguished members of the U.S. Commission on Civil Rights. My name is K.J. Bagchi and I serve as Vice President for the Center for Civil Rights and Technology at the Leadership Conference on Civil and Human Rights. The Leadership Conference is a coalition of 240 plus civil and human rights focused organizations. We recently established a Center for Civil Rights and Technology that will expand and deepen our longstanding work on tech policy issues as we work within our coalition with academics and policy makers to ensure that AI development and other emerging technologies are equitable and beneficial to all communities.

Thank you for the opportunity to testify on this critical topic that has impacted so many constituencies across our coalition. For those in civil society who have been tracking the impact of FRT on communities of color, we have raised a myriad of concerns, but two are worth pointing out here. The first is, this technology is imperfect. In fact, a study by NIST as referenced throughout the day found that FRT is especially likely to misidentify not only Black faces but Native American and Asian faces as well. Second, the use of this technology only further perpetuates biases inherent in the criminal justice

system and other institutions that have had a disproportionate impact on certain races or ethnicities.

Now, in the criminal justice context, the Leadership Conference and Civil Rights Corps have been sounding the alarm on the pervasive and insidious role that facial recognition technologies as well as other tech tools in this arena have had on marginalized communities. Our upcoming policy platform entitled Visions for Justice 2024, calls on the federal government to place a moratorium or outright ban on systems, software, and platforms that further entrench civil rights and civil liberties inequities in the criminal justice system.

Now federal law makers and agencies have also called out failures in deploying this technology. A recent GAO report on the use of FRT within the DOJ and DHS found that the DOJ failed to employ basic measures to protect civil rights. In fact, the GAO report found that most law enforcement officers were not trained before using FRT, and some component agencies lacked specific FRT policies to help protect people's civil rights and civil liberties. The GAO recommended that federal law enforcement agencies including customs and border protection take action to

implement training and policies for civil liberties.

Now, you have heard from many panelists today about how this technology is faulty, how these systems have higher error rates for women and people of color, but it's also important to hear the stories of individuals impacted by the use of this technology. We heard Chair Garza talk about Nijeer Parks who was arrested in February 2019. He faced multiple charges including using a fake ID and shoplifting, but the only evidence that the prosecuting judge had was from an FRT system. Mr. Parks spent 10 days in jail and paid around 5,000 dollars to defend himself. Nine months later, the case was dismissed for lack of evidence.

Another story you heard from Dr. Turner Lee today was from just last year, about Porcha Woodruff, a woman who was eight months pregnant when Detroit police mistakenly arrested her. Ms. Woodruff was held in jail for eleven hours where she started having contractions and had to be taken to the hospital after her release on a 100,000 dollar bond. She was the third person to be falsely identified by FRT in a single police department. What do both of these stories have in common? The victims of misidentification by law enforcement are all Black

individuals, and in each of these instances, police relied heavily on FRT to make an arrest.

Now, given the threat to civil rights and other harms caused by this technology, the arguments for banning or pausing the use of this technology are apparent. However, it is clear that the prevalence of this technology is already widespread, in fact a separate GAO report from last year reported that 20 of 42 federal agencies that employ law enforcement officers use FRT, and thousands of local law enforcement entities have partnered with private companies to develop their own FRT systems, including Clearview AI who you heard from today.

Now, a major question to answer is how agencies are held accountable for the FRT systems they are using. Besides policies and training, it is not clear whether or how the systems that are currently being used are assessed or tested, and how determinations are made to ensure that the FRT use does not threaten civil rights. As such, developing clear guard rails that enhance civil rights protections are much needed.

Now, to that end, the Administration has played a pivotal role in elevating civil rights in artificial intelligence and technology policy through

its executive orders, its public statements, federal guidance and specific policy actions. The OMB draft memo that was referenced in the last panel on AI governance is especially worth noting, and while we in our comments raise a number of concerns with the memo to try to make it stronger, including finding checks on chief AI officers, who can essentially issue waivers on some of the requirements within the memo. We do believe that the memo is notable for its idea of how it implements the idea of rights impacting AI, and how rights impacting AI can trigger risk assessments and mitigation requirements. Under the memo itself, facial recognition activities are considered rights impacting.

Following the directives from this memo, all agencies must implement practices to manage risks from rights impacting and safety impacting FRT. All AI tools, including FRT, must be shown to be safe and trustworthy and that they will produce intended rights-protecting outcomes before it is put into use. We appreciate the Administration's continued commitment to equity and civil rights related to the development of this technology, and we look forward to seeing the final guidance from the OMB to see exactly what enforcing mechanisms look like.

Also, we also want to talk about procurement. Prior to procuring using or funding powerful new technology, agencies must also ensure that the technology actually works. That means that the technology has had sufficient transparent testing to ensure that it will produce intended, fair, equitable, and unbiased results, and does not produce inequitable outcomes for historically disadvantaged groups.

Stopping the use of this technology while guardrails are placed is not a new practice supported by federal agencies. Last year, the Federal Trade Commission came to a settlement with Rite-Aid where the company agreed to cease using facial recognition systems for five years as they addressed its risks. The company is also required to delete any images of consumers collected with the technology and any algorithms developed using such images. Rite-Aid must also notify consumers when their biometric information is processed, and must implement strong data security and providence practices.

Finally, the public has the most to lose from the use of FRT. It is critical that the public interest is represented. As such, agencies should be required to proactively seek community input,

including with civil society and civil rights organizations on their planned use of this technology.

In conclusion, for the use of FRT to be trustworthy, agencies must ensure that the risks are considered early and throughout the AI life cycle. Before procuring or using AI, an agency should understand its limitations and its intended uses before ensuring that the AI tool works for all people and prevent harm. If an FRT platform threatens civil rights, it should be banned.

CHAIR GARZA: Thank you so much Mr. Bagchi. We are going to now hear from Mr. Finch.

MR. FINCH: All right, thank you Chair Garza, fellow commissioners. My name is Brian Finch, and I thank you for the opportunity to speak today about facial recognition technologies and how they might be used by federal agencies. I am a partner at the international law firm of Pillsbury, Winthrop, Shaw, Pittman, here in Washington D.C., but please note that I am here in my personal capacity, and none of my comments reflect the beliefs or positions of any organizations that I have worked with.

Now, let me be perfectly clear. Americans are entitled to a strong expectation of privacy and enforcement of their civil rights. I firmly believe

that, and I am proud to support those rights and expectations in both my career and my volunteer activities. Americans are justified in worrying that facial recognition technologies, FRTs, will erase privacy. We're already closer to a world more recognizable to George Orwell to George Washington, thanks in no small part to the smart phones that act as spies tucked in our purses and pockets. Throw in unchecked usage of FRTs and it with be nigh impossible for anyone to move about their day without leaving some sort of digital record ripe for misuse or abuse.

Still, as I describe below, the worries about the use of FRTs can be mitigated through a combination of rigorous testing and carefully implemented policies. Better still, such mitigation efforts are entirely consistent with America's expectations, because much like any expectation, it is not and cannot be absolute.

I would like to specifically address the fears associated with the federal government's use of so-called 'one to many' matching. As others have noted, FRTs equipped with one to many algorithms are used to compare a captured image of an unknown, unidentified person against a database of photographs of previously identified persons, verified pictures.

The system will then produce a number of possible matches to the unknown person.

It is easy to imagine how a one to many FRT can lead to erroneous results, specifically so-called false positives or mistaken identification of suspects. It is also easy to envision, as others have noted, that flaws in the algorithms will result in unacceptably high false positive rates for specific minority groups, racial groups, genders, and other vulnerable populations. Thankfully though, some federal agencies have already implemented policies that can and should dramatically minimize the possibility of inequitable results.

The Federal Bureau of Investigation, for instance, has in place a series of strict rules that limit the possibility of false positives in its FRT system. Known as the Next Generation Identification Interstate Photo System, NGI IPS. NGI IPS contains criminal mugshots and civil photos submitted with ten print finger prints and offer a facial recognition search capability to law enforcement agencies across the country trying to solve crimes. Importantly, prior to using the NGI IPS, state and local law enforcement officials one, must complete facial recognition training and two, agree to return, and

that the return photos are for investigative lead purposes only, and not a definitive positive identification of the perpetrator of a crime. And rather than returning a single match, NGI IPS also uses an automated process to return up to 50 images, called candidate photos, all of which must be manually reviewed during an investigation.

The Department of Homeland Security's use of facial recognition and face capture technologies directive also provides a useful governance model. The DHS directive prohibits facial recognition technologies from being used as the sole basis for law or civil enforcement related actions, especially investigative leads. Any potential matches or results from the use of facial recognition technology for identification must be manually reviewed by human face examiners prior to any law or civil enforcement action.

Another highly effective way to limit the false positive problem would be to require any and all FRTs used by the federal government to be examined for instance through the National Institute of Standards and Technology's Face Recognition Vendor Testing Program, FRVT, or another widely accepted testing program. Data from that testing program, for

instance, has demonstrated that false positive issues can be limited or eliminated when more accurate algorithms are used. In other words, not all algorithms are the same, and properly vetted ones are effective and protective of civil rights. Understanding that requiring that any federally utilized FRT have a false positive rate below a specified threshold as measured by the testing and agreed upon can minimize if not eliminate concerns about FRTs producing inequitable results for minorities.

Given the above, I would offer the following recommendations to guide the use of FRTs by federal agencies. Number one, require a maximum acceptable false positive rate across racial, ethnic, and gender groups for federal procurements of one to many algorithms, and mandate that any FRT be tested against specified testing programs such as the NIST program. Second, utilize the DHS directive as a basis for federal agency guidelines on the use of FRTs.

That would include A, explicitly acknowledging the security and government/citizen benefits of using FRTs, B, requiring manual human review of any FRT results prior to use in law or civil enforcement actions, and C, include safeguards to

limit the possibility of bias or disparate impact on protected groups, such as by specifying when and for what reason FRTs are used.

Again, I am a strong proponent of privacy, but I also balance that core belief with a recognition that privacy alone cannot be absolute, for when it does become an absolute, criminals will twist that privacy to establish sanctuary from consequences. See for example how child predators share abusing images on end-to-end encryption systems because they know that law enforcement cannot surveil them there. In a similar vein, an absolute prohibition on FRTs by federal government agencies would unnecessarily degrade law enforcement capabilities. The federal government and the nation itself would instead benefit by allowing measured use of FRTs in a carefully controlled manner, and one that balances privacy and security interests.

Thank you for your time, and I look forward to your questions.

CHAIR GARZA: Thank you so much, Mr. Finch. We're going to move on to hear from Dr. Akinwumi.

DR. AKINWUMI: Hi, I'm Michael Akinwumi from the National Fair Housing Alliance, and I'm

grateful to the Commission for the opportunity to speak on behalf of the National Fair Housing Alliance to discuss actions for strengthening responsible federal efforts to practices and policies.

While FRT brings potential benefits to operational efficiency and security within federal government agencies, its use, especially in public housing, presents real concerns for civil rights infringement. For instance, in public housing, the deployment of FRT has led to instances where residents, particularly those from marginalized communities are subjected to invasive surveillance often without their consent.

This policy of monitoring has resulted in a chilling effect on resident privacy and civil liberties, where every move is watched and every visitor is tracked. Such oversight can not only intimidate and stifle free association, but can also lead to wrongful profiling and discrimination. The Atlantic Plaza Towers case in my testimony exemplifies this, where residents felt their privacy was invaded and their civil rights undermined by unwarranted surveillance.

In light of this, we recommend five actions to strengthen responsible federal effort to

practices and policies. One, we recommend implementing stringent testing protocols to ensure FRTs does not result in disparate impact based on race, color, sex, including sexual orientations, national origin, familial status, disability status, and origin. Any FRT system in use must undergo regular assessments, not only for accuracy but also for non-discrimination, with independent and public audits to ensure compliance with fair housing laws and other applicable laws.

Two, we recommend developing strict guidelines around the collection, use, and storage of biometric data, ensuring that residents have clear, informed, consent, and the option to opt out without repercussions. We need federal standards for FRT acquisition, management, development, and oversight. The standards should require agencies including HUD and DOJ to ensure that their FRT use is privacy preserving while providing minimal access to the data required to test the FRT models for discrimination.

Three, we recommend ensuring the physical and psychological safety for all residents in public housing by employing FRT only when there is substantial evidence that it enhances safety without compromising civil liberties, with regular oversight

by an independent body. There should be a continuous assessment and management of potential risks throughout the FRT's life cycle, including the mitigation of unintended and all harmful bias and harmful uses. After deployment, FRT systems should be regularly monitored to ensure they remain safe and effective and to promptly address any issues that arise.

Four, we recommend mandating federal agencies, including DOJ and HUD to be transparent about their use of FRT, including the technology's capabilities, limitations, governance protocols, and the right of those affected to challenge or appeal its use. The National Institute of Standards and Technology must be empowered to issue sector specific recommendations for regulating FRT systems. The Commission must require the publication of governance charters for FRT systems used by federal agencies to provide transparency and accountability information on testing processes, responsible officials, maintenance plans, and downstream impact.

Lastly, we recommend instituting governance frameworks that prioritize human judgements in critical decision-making processes, especially when FRT is employed in areas affecting individual rights,

such as access to housing or essential services. By integrating these policy actions, we can ensure FRT serves the public interest without undermining the civil rights and freedoms we are all committed to protecting. It is not enough to merely employ FRT, how we implement it speaks volumes about our values as a nation committed to civil rights and the rule of law.

To conclude, one, we need to ensure NIST testing of FRT, covers all the five recommendations that I mentioned, we must ensure American leads the world in establishing policies and frameworks that not only advance technological innovations but also guarantee FRT systems uphold civil rights, foster economic growth, and benefit all citizens. It is through such efforts that we can safeguard our collective future in the area of responsible AI, including facial recognition technology. Thank you again for the chance to testify on these critical issues, and I will be happy to take your questions.

CHAIR GARZA: Thank you so much for your testimony, Dr. Akinwumi. We're going to go ahead and hear from Ms. Garvie, if you would proceed, please.

MS. GARVIE: Chair Garza, Vice Chair Nourse and distinguished commissioners, thank you for

inviting me to testify today, I am really honored to be a part of this conversation.

I work with the Fourth Amendment Center at the National Association of Criminal Defense Lawyers, NACDL. We offer training to defense attorneys and expert assistance in cases involving advanced surveillance technologies and tools, where it infringes on people's constitutional rights and liberties. I want to take this opportunity to highlight the impact of facial recognition in the criminal legal system from this defense perspective, and in particular the burden placed on indigent defendants.

Facial recognition has been used in hundreds of thousands of criminal cases for more than 20 years. Rarely is it disclosed to the defense. Given this systematic lack of transparency, law enforcement facial recognition use follows a playbook that is best described as trust, but don't verify. Trust that facial recognition is a reliable way to generate identity leads, but that reliability has never been established. Police facial recognition searches involve a number of human and machine steps, what Deirde Mulligan described as the sociotechnical system, and each of these steps introduce the

possibility of error. Yet the way these searches are run has never been subject to scientifically based peer reviewed study. We quite simply do not know how often these searches in their totality get it right or wrong.

To be sure, the NIST tests that we've heard a lot about and other studies of algorithm performance exist, but these do not reflect the real world conditions in which real people are identified, arrested, and charged. Trust that a facial recognition lead is verified before a search warrant is executed or an arrest is made. Most agencies, as again we've heard today, hold that a facial recognition search produces an investigative lead, not probable cause.

A couple of points on this. One, this is not always, or in my experience working on these cases with defense attorneys, not very often guaranteed. Defendants are frequently identified by a facial recognition search paired only with officer confirmation, a non-witness identification, or some other process that is not legally recognized as a valid ID procedure. Two, even when it is paired with additional investigative steps, there is no guarantee or reliability, as the misidentification of Porcha

Woodruff, Michael Oliver, Alonzo Sawyer, and others show us. And three, further investigative steps do not waive the state's burden to disclose information that is material to the defense.

All of this means that facial recognition often plays a central if not exclusive role in identifying a suspect, and yet rarely do defendants get the opportunity to challenge its use. In many cases, a defendant may never learn that facial recognition was an element of the investigation. In cases where they do, and the defense attorney requests this information under disclosure rules or Brady, they are often told the information isn't discoverable, because it's an investigative lead only, because law enforcement didn't retain the information, because the algorithm is a trade secret belonging to a private company.

For 20-odd years, the facial recognition search process has largely been insulated from judicial scrutiny, has been trusted, but never verified. This systematic lack of transparency is very likely exacerbated by our current plea bargaining system. By some estimates, nearly 98% of criminal convictions come from a plea deal, and when a case involves advanced technology that will give rise to

protractive fights over disclosure or trade secret exemptions, requires highly technical expertise and may involve numerous reliability or other hearings, all while a defendant sits in jail, that person faces what is in most cases insurmountable pressure to plead guilty.

This happens despite claims of guilt or innocence, or of mitigating factors that would come to light during trial. At least two of the men wrongfully arrested because of a facial recognition misidentification considered taking a plea deal to get out of jail more quickly and avoid the trial penalty, the threat of a higher sentence should they take their case to court. This means that the harms of facial recognition, both in terms of due process violations and the risk of misidentification disproportionally impact those overrepresented in the criminal legal system, communities of color and low-income individuals, but particularly indigent defendants.

But the plea bargaining system also serves to further decrease broader transparency into facial recognition use, and this harms the criminal justice system as a whole. When a facial recognition case pleads out, a court never examines the state's burden under Brady to disclose information about how a search

is run, never assesses the reliability of evidence produced by the search under a Frye or Daubert standard, never rules on important legal questions surrounding the use of facial recognition in policing. Instead we remain stuck in this trust but don't verify approach to facial recognition, and due process violations are allowed to persist.

As the Commission examines federal use of facial recognition, it should interpret its mandate broadly, to include federal influence on state and local policing as well. DOJ and DHS are not only facial recognition users, they also provide grants to state and local agencies for the purchase of this and similar advanced technologies, and are actively engaged in policy development, such as through the current process initiated by executive order 14074 on policing, which Deirde Mulligan touched on.

The Commission should also consider how facial recognition may serve as a test case or a cautionary tale for other automated or AI based tools increasingly adopted into modern day policing. If we are ever to realize the goal of the Civil Rights Act, we cannot keep waiting 20 years before examining the civil rights implications of advanced policing technologies and mitigating those harms.

I am grateful for the Commission's attention to these vital issues and look forward to answering your questions.

CHAIR GARZA: Thank you so much, Ms. Garvie, for your testimony. We are going to now hear from our final speaker, Dr. Roff. Please proceed.

DR. ROFF: Commissioners, thank you for the opportunity to present my testimony to you all today regarding civil rights and civil liberties implications for the use of facial recognition technologies by the three agencies we've all been discussing today.

My name is Dr. Heather Roff, and I am providing testimony to you in my private and personal capacity, none of my opinions here represent the Department of Defense, my employers, or anybody I have ever worked for or with.

Before I begin with the points, I'd like to address you all. I'd like to offer a brief explanation as to maybe why my testimony is helpful and slightly unusual to you too. At first blush, my expertise may not seem to be applicable for this particular topic. I am a subject matter expert on issues related to emerging technologies in defense, particularly as how they relate to law, policy, and

ethics. My background is as an ethicist and a social scientist, and much of my work relates to how militaries may or may not use technologies such as artificial intelligence and autonomous weapon systems ethically in war. I have been a leading voice on matters related to lethal autonomous weapon systems, and I was the primary author to the U.S. Department of Defense's AI Ethics Principles that were adopted in February of 2020 by the Secretary of Defense.

Much of my work therefore applies to AI in the context of armed conflict and not in U.S. domestic settings or law enforcement activities. However, given my work, I am very deeply familiar with the ethical implications of technological artifacts in giant bureaucracies. Moreover, I am very familiar with the ways in which mission-driven organizations face bureaucratic challenges in institutional incentive structures that may lead to sub-optimal behaviors of individual members or general outcomes and patterns of behavior that may negatively affect achieving those mission objectives. My comments therefore are directed in this spirit.

For the topic at hand of facial recognition technologies and their use on civil rights, I think we need to think about whether or not

they may achieve their mission objectives or whether and to what extent FRTs on their very own are the underlying issues for the protection of civil rights. Since these three agencies under consideration span a variety of missions, understanding how, where, and under what circumstances the use of FRT is appropriate, is ultimately an exercise in understanding the breadth, the scope, and the operating authorities for each agency.

Law enforcement and domestic national security missions, such as those of DOJ and DHS, are fundamentally different than that of HUD. While there is certainly overlap in joint enterprises between all three, their primary missions are different, and rely on a combination of different assets, tools, policies, and legal regulations at both the federal and state level.

FRT use therefore is looked at as one tool in an arsenal of tools to achieve mission objectives, and yet many reports and experts will attest to this, FRT is not a standalone technology, it is highly dependent on a multitude of factors, such as training data, its representation in quality, and the coupled-ness of the facial recognition system with other information technology systems, databases and humans.

This is because FRT on its own does not provide adequate situational awareness for human operators or decision-makers, and thus require integration with other systems to form what the DOD would call joint command and control.

For example, the ability to identify a person's face may or may not be lawful or useful unless one has not only the authority to operate the sensor, the camera, but also to gather the data into the database who owns that data, query that image against a multitude of data or databases and then place those results against other pertinent facts or contexts, yet where those other facts and context come from can be as varied as, as our colleague from the Miami Police Department noted this morning, social media posts, license plate numbers, geolocations, network associations between individuals identified, demographic information and statistics for the area or region, phone or credit card records, satellite imagery, different language uses and live video feeds from closed circuit television cameras.

The overall situational awareness then provided by the pertinent facts in context is as important as the use of FRT itself, because it's the combinatorial effect of this integration that allows

the agencies to pursue their missions, but also where the limits of those missions are both ethically and legally.

And this is where the difficulty increases, because this is a system of systems, this isn't just facial recognition systems. It's a system of systems. Facial recognition is but one piece, and underlying the entire thing is a mechanical automation IT system that the structure is key to understanding the civil rights implications. But this requires then knowing where the human's place is in that system, and the organization's place in that system. What are the human incentive structures at work? So you can think of that the human incentive structures in that system, you have automation bias, that we've heard about today. You have fatigue, you have memory and recall problems, you have neuroscience and sensory deprivations or even epistemic limitations.

Organizations have incentive structures too. Their missions are obviously one, but the values that are within the organization, and what is valued also leads into what is devalued in that system. What gets hired, fired, and promoted is going to affect how people use facial recognition systems within their organizations. Budgets, time, cost, all of these

types of things are also part of the agency's incentives to use facial recognition. So you have sociotechnical systems, you have human sociotechnical systems, you have humans in the loop, but we don't know what the loop is. So, unless you can actually identify where people are, where systems are, and where individual systems overlap, you are going to face some serious problems in identifying whether or not civil rights implications are at play, if you're just looking at one very small piece of that overall system.

So we have to understand what the tech is doing as well. Facial recognition technology is about pixels, it's pixels as data points, it's a classifier. The structure of the data and its representation is what it's classifying. AI doesn't understand concepts like rights, classes, race, gender, et cetera, it only understands representations and relations in structures in the data. The data is pixels.

I'm running out of time, but basically what I do want to tell you is that these different incentive structures permit and induce different disparate impacts because of the way in which the technology is used in one instance, but also the entirety of the system itself, the system of systems

itself. You have fusion centers and data centers and those things are being used to inform other decisions down the line, but those other decisions down the line are whether or not you have something where the FRT is a lead generator, but how do you define what now is probable cause? It's another automated system that's providing you the evidence that now this is probable cause, but you don't know where in that system anything is human and human-related. I have lots more to say on this, but unless you understand the sociotechnical system of it, and where humans are and where other automated systems are at play, you're never going to unpack the civil rights implications of how it's affecting people on the ground. Thank you.

CHAIR GARZA: Thank you so much, Dr. Roff, and at this point we're going to go ahead and open up the floor to commissioners for questions of this panel. Would anybody like to be recognized first?

COMMISSIONER ADAMS: Not first.

CHAIR GARZA: Not first? I always try to defer and let you all ask questions first, so I don't want to take up too much air time.

COMMISSIONER GILCHRIST: Madame Chair, I'm happy to go first.

CHAIR GARZA: Okay, all right,

Commissioner Gilchrist?

COMMISSIONER GILCHRIST: Thank you all for your testimony today. Mr. Bagchi, I just wanted to ask you to elaborate a little bit more. You mentioned the Rite-Aid situation, do you mind elaborating a little bit more on that, what the issue was with that as it relates to FRT?

MR. BAGCHI: Yeah, definitely. So in that case, it was a commercial use of this technology, and so at Rite-Aid stores, you would have individuals who were being misidentified as shoplifters, and so if they would try to return to the store they would be denied access. You had other complaints where law enforcements was brought in to keep these customers out. And so these complaints were placed with the FTC, and then over time the FTC brought these charges against Rite-Aid.

The issue here, the point I was trying to raise with the Rite-Aid example is that we are able to stop the use of this technology. And so what the settlement found in this case is essentially ordered Rite-Aid to stop using this technology completed, until, for at least five years, and then setting a number of sort of criteria to prove that they are actually handling data correctly, biometric

information correctly, and other risk assessments.

The principles in this settlement are ideas that civil society has been pushing, through legislative means in our responses to OMB AI guidance, and so I use that as an example of where there was concerns raised on the commercial use side, but we can take lessons from that and apply it across the government.

COMMISSIONER GILCHRIST: Yeah, I guess my larger question is, and I guess I can ask this to the entire panel, can we come up with a tool that is not racially biased as it relates to FRT?

MR. BAGCHI: I mean, from our perspective -- oh sorry, I'll just quickly say from the Leadership Conference's perspective, I think when we're looking at institutions that have a history of racial bias and implications, the bar is always, don't use this technology at all, ban it, but again there are ways to test for actual applicability as a secondary, so whether that can happen or not, I'm not, you know, leave it to my other co-panelists, but I would say for us, in institutions in those areas where there has been racial bias, using this technology that has not been proven is not the first step.

COMMISSIONER GILCHRIST: Anybody else want

to weigh in on that?

DR. ROFF: Yeah, so getting back to the actual technical side of it, right, so the technical side is that these systems don't understand what race is. So when you're saying, I'm going to build a facial recognition system to identify as a classifier, is this person, the person in this photo versus this photo, that's what it's doing. And if the relations of the pixels are such that it's following the structure of the data it's fed, and if the data it's fed is structurally racist, you're never going to get a non-racist outcome unless you're trying to bias against it, right? So not all bias is bad in AI, you can bias the other direction, you can try to over represent in another way.

The unfortunate part of this, though, is that with the use of facial recognition in one instance of matching, matching face to face, it's not being supported with just matching, it's being supported with additional facts in context that then are also racially motivated biased and structured, and so the use of facial recognition in those contexts will continue to be racially structured and biased. Does that make sense?

COMMISSIONER GILCHRIST: Sure, absolutely.

CHAIR GARZA: Dr. Akinwumi?

DR. AKINWUMI: Yes. So I have two quick reactions. One, I think it's not completely true to say the system does not understand what race is. Even if you just look at the data itself, like the pixels that my co-panelist referred to, it's more or less suggesting that other protected classes like color, sex, sexual orientations, are not something that can be inferred by FRT, right? That said, we know for a fact that when it comes to developing any AI system, when the underlying data is imbalanced, when there is a representation issue in the underlying data, then we need rigorous testing, just like Brian said, to address or mitigate many of the associated risks.

So the panel before mine, Laura from UnidosUS said that we know that, when we talk about marginalized communities, or people of color, so even if we try to use the underlying images to reflect or mirror the demographics that we have in the U.S., the underlying data, there will always be under-representation. So it's fair to say that even if you have a perfect data that is representing the demographics that we have currently, along all the protected classes, and we also have perfect algorithms, the underlying efforts is like the

convolution on neuro networks and other limited technologies, we will always have this issue of bias. Even if we agree, there's an agreement on what errors we want to prioritize, in prior panels we've heard about false positive, false negative, these are just examples or instances of error metrics, even if there is an agreement on which ones to standardize, there will always be differences or discrepancies, and that is where having a human in the loop is very, very important, that we have human judgement to evaluate these decisions that are coming out of the system.

So even though we have all these protected classes that are all being used in the training or in the modeling, but having a human in the loop, who'd actually check these outcomes along lines like disability status, along lines like color and race, even though they are not in the underlying input that is going into the system.

COMMISSIONER GILCHRIST: Thank you, Madam Chair, I appreciate that.

CHAIR GARZA: Of course. And just a follow up question, I guess generally, is understanding the bias within these systems, are there any mechanisms that we're aware of to de-bias the technology? And I'll leave that open.

DR. AKINWUMI: I will use examples of mortgage underwriting to answer your question. So we know for example when it comes to mortgage underwriting, there are techniques out there for de-biasing all the components of AI systems. Essentially, if you think of any AI system including FRT, there are three components. You have the data, you have the algorithm itself, and the output. And right now, when it comes to FRT, I think we can invest in research to look into how the underlying data, which powers the FRT systems, and the architecture of the models themselves can be constrained to limit the bias that is coming out of the system, even when you have underrepresented systems.

So in other areas there are techniques for constraining or limiting the bias, but when it comes to FRT, we need significant investment when it comes to doing the research to invent or find these techniques to address under-representation issues to address the model itself.

MR. FINCH: Chair Garza, allow me to draw an analogy. I fly up from my home in Charleston, South Carolina, regularly, here to Washington D.C., and so I must go through magnetometers and millimeter wave scanners on a regular basis. If you are

unfortunate enough to be caught in a TSA line for more than a few minutes, you will notice occasionally that the TSA screeners are regularly calibrating those machines, and they will also be sending test packages through those devices as well in order to verify that they are working as intended.

To your question then, when we are talking about possible controls in order to eliminate bias, and recognizing past testimony about issues with the actual use in the field, the lighting conditions, quality of images, et cetera, I would argue, based on research I've conducted in the past, it's not just the initial testing that we've discussed before, and it could be NIST, I could be other organizations who've come up with the initial test, an important recommendation would be continued auditing of these systems after their deployment in order to ensure that they are meeting the benchmarks, whatever they may be, so that there is continued confidence in these systems that bias is, I would say most likely drastically limited, probably not eliminated, because it's difficult to eliminate any bias in any system. And people have their own biases, technologies can have errors in them, coding errors, I'm a lawyer because I can't do math or code so please don't put me in charge

of any of these systems.

But my simple point is that to your question, yes, I do think there are ways to mitigate these, but it has to be viewed as a continuous process, even to the point that Clare Garvie made earlier, I think that would include disclosure and transparency in the system. And if we're talking specifically here on this panel, about federal use of facial recognition technologies, that would be an important requirement in guidance or directives to agencies, that there is transparency when it is being used for law enforcement purposes, and that that information is being presented to the defendant or the suspect in this case.

As Dr. Roff put it, and I think this is probably the best way I've heard it be phrased, facial recognition should be viewed as a lead generator. And that should be its main purpose, to be followed by human intervention, human review, and continuous auditing.

DR. ROFF: Can I just -- one thing around that, real quickly. The idea about accuracy has taken up the lion's share of I think the time today, in whether or not things are accurate, or whether they are biased, and those are two actually, can be

different questions, right? So accuracy however is a really easy objective to meet technically, right, we can test for accuracy in the system, in house. In the wild uses, accuracy is going to go down. We see that across the board, and DOD applications say of facial recognition systems, which the DOD uses as well, the accuracy goes down, right, because if you're in a jungle versus a desert versus an urban environment, all of these things matter, right?

So I think when you say accuracy goes down depending upon context, therefore we need continual testing and evaluation, verification validation, continual testing, that's what is being argued for. However, continued T&E and V&V is really, really hard, and it's really, really expensive. And so when we're talking about doing continuous T&E and V&V, that too is an automated tool. If you do continuous testing, that continuous testing is also an automated tool. So you have to make sure that your automated tool that's testing your automated tool is equally good or better, and right now I don't know if we have that. As well as the cost in effective guidance that we need and the money we need to roll that continuous testing with facial recognition technologies.

These institutions, these agencies, are

already really extremely on tight budgets, and I can't imagine them engaging in more money spending for continuous testing or continue with audit trails and things like that, and continual bureaucratic overhead. So you'd have to think about ways in which are likely that they would do that.

CHAIR GARZA: Go ahead.

COMMISSIONER JONES: So Dr. Roff, do you then support the moratorium on FRT that is supported by the Leadership Conference? I mean you take a very dim view of FRT and I kind of want to get to your conclusions on the usefulness of it at all, I guess.

DR. ROFF: I take a dim view on the use of FRT fused with lots of other different things for the proof of an illegal or an illicit act happening. So if my face comes up and it says, you know, Mr. Jones, 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, 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.

COMMISSIONER JONES: Okay, so I appreciate the amendment to that. But it sounds like you take the view that is hopeless, that it is irreparable because of what you've described as intrinsic biases. And so is it that you advocate not using it in the law enforcement context, where the stakes are so high? And maybe in the HUD context, too, where I also have a lot of concerns.

DR. ROFF: I would take it with a very large grain of salt and I would add more boots on the ground requirements for investigative officers to generate leads through other, what we would call in the DOD dual phenomenology. So if I have evidence of an incoming nuclear missile, I need to make sure that I have multiple different kinds of sensors telling me the same thing, right? But if I have all the information coming from the same set of sensors, I can't rely on that.

So in the facial recognition kind of course, I want to have information that I'm relying on that has nothing to do with all of these automated

processes. And so when we talk about humans in the loop, we need to know what the loop is, right? 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, right, 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 judgement when looking at that system.

So I would say we can utilize these systems but we have to 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.

CHAIR GARZA: Well that gave me a lot to think about. I mean, do you want to -- I was going to say, I want to go in like a different direction towards discussing, bringing Ms. Garvie in on criminal issues.

COMMISSIONER MAGPANTAY: I have questions there too, but let me -- I think that actually, Mr. Finch actually raised some of those issues and you know, I just want to note also for the record that I appreciated the recommendations and I appreciated the structure of the testimony. I mean trainings, using the technology as investigatory leads, not to

establish culpability, the human verification, the need for warrant, I read it and it was excellent. I think that those are the safeguards that we are looking at.

Two questions for Mr. Finch. One, the 2023 DHS directive, would you recommend that directive for other agencies? And I'll just ask the second question, you talked about a maximum rate, there should be a maximum rate, I've got to ask, so what is that rate?

MR. FINCH: I am not qualified.

COMMISSIONER MAGPANTAY: I know, but could you take a guess?

MR. FINCH: I would say it's very low, meaning under one percent, very low under one percent, and that is an absolute guess, and I also would defer to what that number actually is in part with the informed judgement of this group, these commissioners, for something that you would feel comfortable with.

COMMISSIONER MAGPANTAY: Well we're asking you, you think we know?

MR. FINCH: I am a lawyer, so I'm going to ask questions in response to questions, but no, I think it's going to be very sub one percent. And that is in recognizing again, that I am a strong advocate

for additional verification and that this is just a lead generator, right? And that I am in support of returning 20, 30, 40, 50 pictures that an investigator then can utilize to make a further determination, being mindful again, for instance, of Ms. Garvie's testimony, which I think is very enlightening and I think hyper-relevant in that regard.

With respect to the DHS guidance, I think it is a good basis template for other federal agencies to utilize with respect to the limitations of how they can use facial recognition technologies for identification purposes, its limitations on only being, again, a lead generator, requiring manual intervention, human intervention, afterwards as well. I do want to add though that I'm not necessarily saying that every cabinet agency, every executive branch agency should be using facial recognition technologies for identification purposes.

I would say that's number one, probably beyond the scope of my testimony but number two, I don't know that for instance the Department of Agriculture is going to be needing to use facial recognition technologies widely, maybe at some of their facilities where they're doing biodefense research for instance, it might be useful in that

case, for surveillance purposes to protect those grounds, but I also think that it is worth a discussion to say, is this properly only for the Justice Department, for Department of Homeland Security, for Department of Defense to use for their criminal investigatory premises or for perimeter protection. Beyond that, again I think it is worth a discussion saying, reaching the point of saying, is any risk of bias too much? And if so, then maybe this isn't the right technology for every federal agency.

COMMISSIONER MAGPANTAY: And I just need to get this -- that was an excellent point, because you just reminded me, so an immigration violation is not punishment for a law, and therefore the constitutional protections that we all learned in law school do not apply and attach. Therefore, the standards are higher in a criminal investigation for the FBI, it's lower for immigration.

Thank you professor, for reminding -- no, no, I wanted to put that down because I was going the other way, but this is very helpful in understanding why it would not -- the DHS policies are helpful but are inherently insufficient because they do not provide the constitutional standards that are required in a criminal investigation that the FBI and other law

enforcement would require. Thank you very much.

CHAIR GARZA: Yeah, and that's kind of where I wanted to bring you in, Ms. Garvie, is just thinking about those, the criminal law implications of this. I mean, what's more precious than someone's freedom? And we've heard testimony earlier today as well as on this panel just how much harm can come from a false positive, from being dragged into court. This body has heard multiple reports from our state advisory committees about just what happens when someone goes through the criminal justice system and they're exonerated, they still have something on their record that they have to expunge. And I also know that from practicing criminal defense law, just that's not part, you know, that's something that you have to pay for out of pocket as an individual.

So I wanted to bring you into this conversation and just, you know, what do you see here as the potential? I mean, considering the tension with constitutional protections that one would normally get in a criminal defense.

MS. GARVIE: Sure. So I'm going to say at the outset that NACDL's position is that facial recognition should not be used in the criminal investigative context because of all the harms and

because of the 20-odd years of due process violations that its use has represented and continues to represent.

The harms are of misidentification, but they are broader than that, and that's the systematic deprivation of due process rights to defendants, whether or not they're innocent, they are still entitled to information, potentially exculpatory information, information material to their defense that the prosecution has, and face recognition falls into that.

This line that face recognition is an investigative lead only comes up a lot, and you hear it from basically every single law enforcement agency. And in theory, that is a valuable check against misidentification, but we have to be cautious against over-relying on that for a couple of reasons. One is, what does it mean? Is it sufficient for an officer who is not a witness to the crime to look at two photos and say that is the same person? That is not a cognizable ID procedure, so I would argue no. But we see that, we see the interpretation of investigative lead only, additional investigative steps need to be taken as amounting to something as little as that.

Or in the Robert Williams case, showing

the video of the robbery to a non-eye-witness and asking that non-eye-witness to perform an eye-witness function of viewing a six pack and performing an identification. Again, an assumption is being made that the additional investigative steps are going to be reliable, independent, and somehow corroborate as opposed to confuse the identity process.

I also want to flag that I think well-meaning legislatures often look at this investigative lead only as a directive to tell law enforcement not to include face recognition in their arrest warrant application, to sort of not disclose it to the judge, because it shouldn't affect whether or not an arrest warrant is made. But what happens if it's not in that arrest warrant application, is that the defense literally never finds out that it was used. That is often the only place, and it is rarely in there, but it will be the only place that it shows up. So this lack of transparency is hugely problematic in this investigative lead only concept, really feeds into that and perpetuates it.

CHAIR GARZA: Would you liken it to, not a witness, somebody who is, the colloquial term is a snitch, somebody who is identifying someone for police, is it the same kind of situation, is that

comparable here?

MS. GARVIE: That's a question for courts. Yes, how much weight to give a face recognition possible match, or that investigative lead, is fundamentally a question that judges should be answering, the probable cause threshold. I would say on this point -- actually I've lost my train of thought, my apologies, I'll get back to you if I get it.

CHAIR GARZA: Commissioner Jones, go ahead.

COMMISSIONER JONES: So for Ms. Garvie, can you walk me through an example where using a set of hypothetical or maybe real life facts where there would be prejudice to a defendant, where there is a warrant that is issued, but the application for the warrant does not indicate a reliance on facial recognition technology and defense counsel is unable to challenge that? I'm trying to wrap my mind around the prejudice in the omission of that, because I imagine that if that data is being omitted that there's still other facts being alleged in the application for the warrant that the judge would find sufficient to grant the warrant. So can you just help me with that please?

CHAIR GARZA: If I can jump in, it's informant, that's the word I was looking for. It's like, is it comparable to an informant, and do you see informants disclosed on, in the same way that maybe facial recognition technology would be, to add to Commissioner Jones's question.

MS. GARVIE: Great, so I'm going to take that point real quickly, because I think they do connect. And this is a fundamental question of reliability. Is it equivalent to a confidential informant? We don't have the answer to that question because we don't know the foundational validity of facial recognition as applied. We actually don't know how reliable the face recognition search process is.

The reason why I say that is because it has at least four human subjective decision-making points in each face recognition search. Is the probe photo, the photo of the unknown individual good enough for running through a face recognition search? Am I going to edit the photo before submitting to an algorithm? That is not uncommon. And then, looking at the candidate list. Is there a person that matches my probe photo in this candidate list? How many of those photos am I going to look through? Can I look at additional information, what we call task

irrelevant information for other biometric investigative techniques. Can I look at whether this person has been arrested previously for a similar crime while I'm conducting a biometric face comparison?

So these are all areas that have not really been robustly tested, either individually or as a whole, so I can't really answer the question of whether face recognition result is equivalent to a confidential informant, because we don't have an answer to that. And I would defer to researchers, to computer scientists, and to cognitive psychologists to answer that question.

In terms of your hypothetical, I think the Nijeer Parks case is a really interesting example. Nijeer Parks was misidentified as being present at a robbery and then sort of aggravated assault, as the suspect sped away, he attempted to hit an officer with his vehicle. The way that Nijeer Parks was identified was through a face recognition match that then an officer looked at the fraudulent Tennessee driver's license that was left at the scene of the crime and Nijeer Parks's mugshot and said that's the same person. A court said that was sufficient probable cause.

COMMISSIONER JONES: So a search a done, there was a positive, and then the police officer independently looked at the driver's license and compared it to the face that the FRT matched with?

MS. GARVIE: Yep, he did a one-to-one comparison. He was not a witness to the crime. We don't know how good he is at looking at two faces and determining whether they represent the same person. That was the only additional corroborative steps, and it wasn't sufficient to correct for the misidentification that took place. And that's pretty common, I've got to say, in looking at the cases that I'm involved in on a day-to-day basis, that is not an exception, that type of fact pattern.

CHAIR GARZA: I mean that makes me think about the prior panel where we heard about the history of film development and kind of these databases having these older photos that don't necessarily show the features of darker skinned folks, I mean, that seems like a factor here as well, depending on what database you're looking at or what kind of photo you have in front of you. Dr. Roff?

DR. ROFF: Yeah, I just wanted to bring up the attention, I haven't heard it today, and that could be my own hearing problem, but you know, the

Harvey Murphy Jr. case of this year, where Mr. Murphy is in Texas, he's 61 years old, he was arrested on a warrant for theft of something at Sunglasses Hut, right? Unfortunately, Mr. Murphy was not present in Texas at the time of the theft, and a warrant was issued for his arrest based on facial recognition from video camera feed in the Sunglass Hut store. When Mr. Murphy came back to Texas to renew his driver's license, there was a warrant for his arrest, he was subsequently arrested, he was then placed into jail, and while he was awaiting somebody to de-conflict the problem that he was not present in Texas at this time and could not be there for the person that was identified through FRT, he was subsequently physically and sexually assaulted in prison, and then he was let go several days later, but unfortunately the physical and sexual abuse had already taken place. And now he's suing Macy's, the owner of Sunglass Hut for 10 million.

I haven't heard anything about lawsuits against Houston Police Department and what the judge would have required in a case of a one-to-one match or anything else. All that's been reported to date that I know of is that the loss prevention person said that that's the guy, and that was sufficient enough for

them with the facial recognition and the loss prevention officer telling the police. So that is another area where you go, humans aren't so great.

COMMISSIONER MAGPANTAY: Excellent. So Ms. Garvie, I actually really appreciated the walk through, and the four elements of subjectivity. It would seem to me that the defense counsel should be entitled to that information too, if the police have it, certainly the defense should have it. Ms. Roff's question, Ms. Roff's example actually helps me to re-raise a question that I asked the last panel. So there are mistakes, people are put into jail wrongfully and it's -- I wanted to ask you about redress. Ted Lieu talked about a private right of action, somebody suing, are there sufficient safeguards, we had another panelist who said if the government makes the mistake they should compensate, you know, false imprisonment standard, why does that not work? Can you just, assume that it happens, someone is wrongfully arrested, wrongfully detained, I understand that they can file a lawsuit. What other safeguards can we provide so that the victim can be appropriately compensated and redress is provided. Ms. Garvie?

MS. GARVIE: That is a great question. I

do not work in the civil space, so that is not something I contemplate a lot beyond recommending the private right of action should somebody be unfortunately wrongfully accused.

COMMISSIONER MAGPANTAY: All right. Anyone?

MR. FINCH: I would note, in this civil context and in the state context, two states for instance that have passed very strict biometric privacy laws, California and Illinois. And I apologize, I wasn't here all day so I don't know if that had been discussed earlier, but those are two states where there is a right of redress, and in that case for collecting of biometric information which can include face, fingerprints, gait, other unique identifiers, et cetera.

And there has been, shall we say, a tremendous amount of litigation associated with that for the improper or improperly disclosed collection of that information by individual businesses. And I'm not necessarily saying that that is the appropriate solution, because a number of my friends on the plaintiff's bar are very active in that area, shall we say, when it comes to enforcing that law, which is consistent with its intent, however I do want to note

that at least when it comes to the collection of the information, so your inter database, there are states that have taken the lead. And Europe has as well, I mean the European Union through general data protection regulation, about collecting of your information to be in a database and your right to request deletion, et cetera.

COMMISSIONER MAGPANTAY: Thank you.

CHAIR GARZA: No final questions? Commissioners on the phone, do you all have any questions?

VICE CHAIR NOURSE: No questions from me.

CHAIR GARZA: Okay, wonderful. Well, I would like to thank our panelists for your time, for your testimony, and for the robust conversation. I know some of us probably have more questions now, after hearing all of this, it's been a really great, wonderful day, so that brings us to the end of our briefing.

Again, thank you to everyone who attended in person as well as online, and again thank you to the staff for all your hard work in making sure that everything runs smoothly and that we are on time. And on behalf of the entire Commission, thank you.

And as a reminder, for this briefing, the

record is going to remain open until April 8, 2024. Panelists or members of the public who would like to submit materials for the Commission's consideration, which we welcome, may mail them to the U.S. Commission on Civil Rights, Office of Civil Rights Evaluation, 1331 Pennsylvania Avenue Northwest, Suite 1150, Washington D.C., 20425, or you can email them to frt@usccr.gov.

I ask that our attendees move any continuing conversations outside of the hearing room so our staff can complete any logistics necessary to close out, and please make sure you exit the building through the F Street lobby, as the exit to the Pennsylvania Avenue if you did not know already is closed.

So having concluded this public briefing on the civil rights implications of the federal use of facial recognition technology, I hereby adjourn this briefing at 4:31 p.m. Eastern Time. Thank you all.

(Whereupon, the above-entitled matter went off the record at 4:31 p.m.)