FACIAL RECOGNITION TECHNOLOGY (PART III): ENSURING COMMERCIAL TRANSPARENCY AND ACCURACY

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

JANUARY 15, 2020

Serial No. 116–82

Printed for the use of the Committee on Oversight and Reform

Available on: *http://www.govinfo.gov*
oversight.house.gov or
docs.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
39–581 PDF WASHINGTON : 2020

COMMITTEE ON OVERSIGHT AND REFORM

CAROLYN B. MALONEY, New York, *Chairwoman*

Eleanor Holmes Norton, District of Columbia
Wm. Lacy Clay, Missouri
Stephen F. Lynch, Massachusetts
Jim Cooper, Tennessee
Gerald E. Connolly, Virginia
Raja Krishnamoorthi, Illinois
Jamie Raskin, Maryland
Harley Rouda, California
Debbie Wasserman Schultz, Florida
John P. Sarbanes, Maryland
Peter Welch, Vermont
Jackie Speier, California
Robin L. Kelly, Illinois
Mark DeSaulnier, California
Brenda L. Lawrence, Michigan
Stacey E. Plaskett, Virgin Islands
Ro Khanna, California
Jimmy Gomez, California
Alexandria Ocasio-Cortez, New York
Ayanna Pressley, Massachusetts
Rashida Tlaib, Michigan
Katie Porter, California
Deb Haaland, New Mexico

Jim Jordan, Ohio, *Ranking Minority Member*
Paul A. Gosar, Arizona
Virginia Foxx, North Carolina
Thomas Massie, Kentucky
Mark Meadows, North Carolina
Jody B. Hice, Georgia
Glenn Grothman, Wisconsin
James Comer, Kentucky
Michael Cloud, Texas
Bob Gibbs, Ohio
Clay Higgins, Louisiana
Ralph Norman, South Carolina
Chip Roy, Texas
Carol D. Miller, West Virginia
Mark E. Green, Tennessee
Kelly Armstrong, North Dakota
W. Gregory Steube, Florida
Fred Keller, Pennsylvania

David Rapallo, *Staff Director*
Yvette Badu-Nimako, *Senior Counsel*
Courtney French, *Senior Counsel*
Gina Kim, *Counsel*
Alex Kiles, *Counsel*
Amy Stratton, *Deputy Chief Clerk*
Christopher Hixon, *Minority Staff Director*
Contact Number: 202-225-5051

CONTENTS

WITNESSES

Opening statements, and prepared statements for the witnesses are available at: docs.house.gov.

INDEX OF DOCUMENTS

The documents listed below may be found at: docs.house.gov.

FACIAL RECOGNITION TECHNOLOGY (PART III): ENSURING COMMERCIAL TRANSPARENCY AND ACCURACY

Wednesday, January 15, 2020

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND REFORM,
SUBCOMMITTEE ON ECONOMIC AND CONSUMER POLICY,
Washington, D.C.

The committee met, pursuant to notice, at 10:02 a.m., in room 2154, Rayburn House Office Building, Hon. Carolyn B. Maloney, presiding.

Present: Representatives Maloney, Norton, Lynch, Cooper, Connolly, Krishnamoorthi, Kelly, DeSaulnier, Lawrence, Plaskett, Khanna, Gomez, Ocasio-Cortez, Pressley, Tlaib, Haaland, Jordan, Foxx, Massie, Meadows, Hice, Grothman, Comer, Cloud, Higgins, Miller, Green, Armstrong, Steube, and Keller.

CHAIRWOMAN MALONEY. The committee will come to order.

Good morning, everyone. And without objection, the chair is authorized to declare a recess of the committee at any time. With that, I would now like to recognize myself to give an opening statement.

Today, the committee is holding our third hearing this Congress on a critical issue, facial recognition technology. It is clear that despite the private sector's expanded use of technology, it is just not ready for primetime. During this hearing, we will examine the private sector's development, use, and sale of technology, as well as its partnerships with government entities using this technology.

We learned from our first hearing on May 22 of 2019 that the use of facial recognition technology can severely impact Americans' civil rights and liberties, including the right to privacy, free speech, and equal protection under the law. We learned during our second hearing on June 4 how Federal, state, and local government entities use this technology on a wide scale, yet provide very little transparency on how and why it is being used or on security measures to protect sensitive data.

Despite these concerns, we see facial recognition technology being used more and more in our everyday lives. The technology is being used in schools, grocery stores, airports, malls, theme parks, stadiums, and on our phones, social media platforms, doorbell camera footage, and even in hiring decisions, and it is used by law enforcement. This technology is completely unregulated at the Federal level, resulting in some questionable and even dangerous applications.

On December 2019, the National Institute of Standards and Technology issued a new report finding that commercial facial recognition algorithms misidentified racial minorities, women, children, and elderly individuals at substantially higher rates. I look forward to discussing this study with Dr. Romine, the Director of NIST's Information Technology Laboratory, who is joining us today. I also look forward to hearing from our expert panel hailing from academia, industry, and the advocacy community on recommended actions policymakers should take into account to address potential consumer harm based on these findings.

Our examination of facial recognition technology is a bipartisan effort. I applaud Ranking Member Jordan's tireless and ongoing advocacy on this issue. We have a responsibility to not only encourage innovation, but to protect the privacy and safety of American consumers. That means educating our fellow members and the American people on the different uses of the technology and distinguishing between local, subjective, identification, and surveillance uses. That also means exploring what protections are currently in place to protect civil rights, consumer privacy, and data security and prevent misidentifications, as well as providing recommendations for future legislation and regulation.

In that vein, I would like to announce today that our committee is committed to introducing and marking up common sense facial recognition legislation in the very near future. And our hope is that we can do that in a truly bipartisan way. We have had several conversations, and I look forward to working together toward that goal.

I now recognize the distinguished Ranking Member Jordan for his opening statement.

Mr. JORDAN. Thank you, Madam Chair. We appreciate your willingness to work with us on this legislation. We have a bill that we will want to talk about as well.

Facial recognition is a powerful new technology that is being widely used by both government agencies and private sector companies. Its sales have experienced a 20 percent year-to-year growth since 2016, and the market is expected to be valued at $8.9 billion by 2022.

Increasingly, local, state, and Federal Government entities are utilizing facial recognition technology under the guise of law enforcement and public welfare, but with little to no accountability. With this technology, the Government can capture faces in public places, identify individuals, which allows the tracking of our movements, patterns, and behavior. All of this is currently happening without legislation to balance legitimate Government functions with American civil liberties. That must change.

And while this hearing is about commercial uses of facial recognition, I want to be very clear. I have no intention of unnecessarily hampering technological advancement in the private sector. We understand and appreciate the great promise that this technology holds for making our lives better. It is already improving data security and leading to greater efficiency in verification and identification that prevents theft and protects consumers.

The urgent issue, the urgent issue we must tackle is reining in the Government's unchecked use of this technology when it impairs our freedoms and our liberties. Our late chairman, Elijah Cummings, became concerned about Government use of facial recognition technology after learning it was used to surveil protests in his district related to the death of Freddie Gray. He saw this as a deeply inappropriate encroachment upon the freedoms of speech and association, and I couldn't agree more.

This issue transcends politics. It doesn't matter if it is a President Trump rally or a Bernie Sanders rally, the idea of American citizens being tracked and catalogued for merely showing their faces in public is deeply troubling. It is imperative that Congress understands the effects of this technology on our constitutional liberties.

The invasiveness of facial recognition technology has already led a number of localities to ban its government agencies from buying or using digital facial recognition for any purpose. This trend threatens to create a patchwork of laws that will result in uncertainty and may impede legitimate uses of the technology. Unfortunately, this is not an issue we should leave to the courts. Facial recognition presents novel questions that are best answered by congressional policymaking, which can establish a national consensus.

The unique Government-wide focus of this committee allows us to consider legislation to address facial recognition technology here at the Federal level. We know that a number of Federal Government agencies possess facial recognition technology and use it without guidance from Congress, despite its serious implications on our First and Fourth Amendment rights. At the bare minimum, we must understand how and when Federal agencies are using this technology and for what purpose. Currently, we do not know even this basic information.

Because our committee has jurisdiction over the entire Federal Government's use of emerging technology, we must start by pursuing policy solutions to address this fundamental information. It is our intention as well to introduce legislation. We are trying to work with both sides here, trying to work together. That will provide transparency and accountability with respect to the Federal Government's purchase and use of this technology and this software. I am pleased to be working with my colleagues across the aisle on the bill that would address these questions.

And again, I want to thank you, Madam Chairwoman. And I look forward to hearing from our witnesses today and thank them for being here. I yield back.

Chairwoman MALONEY. Thank you, Mr. Jordan.

But before we get to the witnesses, I would like to make a unanimous consent request. I would like to insert into the record a report from the ACLU, which found that Amazon's recognition technology misidentified 28 Members of Congress as other individuals who had been arrested for crimes, including John Lewis, a national legend, a national civil rights leader. So, I would like to place that into the record.

Chairwoman MALONEY. And I would also like to mention that three members of this committee were misidentified, Mr. Gomez, Mr. Clay, and Mr. DeSaulnier. And they were misidentified—that shows this technology is not ready for primetime—along with 11 Republican Members of Congress.

So, I would now like to recognize my colleague Mr. Gomez, who has personal experience with this, for an opening statement.

Mr. GOMEZ. Thank you, Madam Chair.

First, this is the committee is holding its third hearing on this issue, and up until two years ago, this issue was not even on my radar, until the ACLU conducted this test, which falsely matched my identity with somebody who committed a crime. Then all of a sudden, my ears perked up. But I had no doubt that I was misidentified because of the color of my skin than anything else.

So, as I started to learn and do research on this issue, my concerns only grew. I found out that it is being used in so many different ways. Not only in law enforcement—at the Federal level, at the local level—but it is also being used when it comes to apartment buildings, when it comes to doorbells, when it comes to shoppers, when it comes to a variety of things, right? But at the same time, this technology is fundamentally flawed.

For somebody who gets pulled over by the police, in certain areas, it is not a big deal. In other areas, it could mean life or death if the people think you are a violent felon. So, we need to start taking this seriously.

This issue probably doesn't rank in the top three issues of any American out in the United States, but as it continues to be used and it continues to have issues, there will be more and more people who are misidentified and more and more people who are questioning if their liberties and their freedoms are starting to be impacted for no fault of their own, just some algorithm misidentified them as somebody who committed a crime in the past.

So, this is something that we need to raise the alarm. And that is what these hearings are doing in a bipartisan way. To make sure that the American public doesn't stumble into the dark, and suddenly, our freedoms are a little bit less, our liberties are a little bit less. So, we will start having these important discussions in a bipartisan way to figure out how and what can the Federal Government do. What can Congress do? What is our responsibility?

And with that, I appreciate the chair's commitment to legislation. I also appreciate the ranking member's commitment to legislation because I know that this issue is a tough one, and it only could be done in a bipartisan way.

With that, I yield back.

Chairwoman MALONEY. I now recognize Mr. Meadows of North Carolina for an opening statement.

Mr. MEADOWS. Thank you, Madam Chairman and the ranking member, both of you. Thank you for your leadership on this important issue.

Two things that I would highlight. Certainly, we know Mr. Gomez, and we know that there is certainly no criminal background that he could ever be accused of being involved with. And so, I want to stress that his character is of the utmost as it relates to even us on this side of the aisle.

And I say that in jest because one of the things that we do need to focus on—and this is very important to me, I think that this is where conservatives and progressives come together—and it is on defending our civil liberties. It is on defending our Fourth Amendment rights, and it is that right to privacy. I agree with the chairwoman and the ranking member and Mr. Gomez and others on the other side of the aisle, where we have had really good conversations about addressing this issue.

To focus only on the false positives I think is a major problem for us, though, because I can tell you, technology is moving so fast that the false positives will be eliminated within months. So, I am here to say that if we only focus on the fact that they are not getting it right with facial recognition, we have missed the whole argument because technology is moving at warp speeds, and what we will find is, is not only will they properly—my concern is not that they improperly identify Mr. Gomez, my concern is that they will properly identify Mr. Gomez and use it in the wrong manner.

So, for the witnesses that are here today, what I would ask all of you to do is, how can we put a safeguard on to make sure that this is not a fishing expedition at the cost of our civil liberties because that is essentially what we are talking about. We are talking about scanning everybody's facial features, and even if they got it 100 percent right, how should that be used? How should we ultimately allow our Government to be involved in that?

I am extremely concerned that as we look at this issue that we have to come together in a bipartisan way to figure this out. I think it would be headlines on the, you know, New York Times and Washington Post if you saw Members of both parties coming to an agreement on how we are to address this issue. I am fully committed to do that.

Madam Chair, I was fully committed to your predecessor. He and I both agreed at the very first time where this was brought up that we had to do something. And I know the ranking member shares that. So, I am fully engaged. Let's make sure that we get something and get something done quickly, and if we can do that, you know?

Because I think if we start focusing again on just the accuracy, then they are going to make sure that it is accurate, but what standards should we have the accuracy there? Should it be 100 percent? Should it be 95 percent? You know, I think when Mr. Gomez was actually identified, the threshold was brought down to 80 percent. Well, you are going to get a lot of false positives when that happens, but we need to help set the standards and make sure that our Government is not using this in an improper fashion.

With that, I yield back.

Chairwoman MALONEY. I thank the gentleman for his statement.

I would now like to introduce the witnesses. We are privileged to have a rich diversity of expert witnesses on our panel today. Brenda Leong is a senior counsel and Director of AI and Ethics at the Future of Privacy Forum. Dr. Charles Romine is the Director at the Information Technology Laboratory of the National Institute of Standards and Technology.

Meredith Whittaker is the co-founder and Co-Director of the AI Now Institute at New York University. Daniel Castro is the vice president and Director of Center for Data Innovation of the Information Technology and Innovation Foundation. And Jake Parker is the Senior Director of Government Relations at the Security Industry Association.

If you would all rise and raise your right hand, I will begin by swearing you in.

Do you swear or affirm that the testimony you are about to give is the truth, the whole truth, and nothing but the truth, so help you God?

[Response.]

Chairwoman MALONEY. Let the record show that the witnesses all answered in the affirmative. Thank you, and please be seated.

The microphones are very, very sensitive, so please speak directly into them. And without objection, your written testimony will be made part of our record.

With that, Ms. Leong, you are now recognized for five minutes.

STATEMENT OF BRENDA LEONG, SENIOR COUNSEL AND DIRECTOR OF AI AND ETHICS, FUTURE OF PRIVACY FORUM

Ms. LEONG. Thank you for the opportunity to testify and for considering the commercial use of facial recognition technology.

This is an important challenge. The Future of Privacy Forum is a nonprofit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. We believe that the power of information is a net benefit to society and that it can be appropriately managed to control the risks to individuals and groups.

Biometric systems, such as those based on facial recognition technology, have the potential to enhance consumer services and improve security, but must be designed, implemented, and maintained with full awareness of the challenges they present. Today, my testimony focuses on establishing the importance of technical accuracy in discussing face image-based systems, considering the benefits and harms to individuals and groups, and recommending express consent as the default for any commercial use of identification or verification systems.

Understanding the specifics of how a technology works is critical for effectively regulating the relevant risks. Not every camera-based system is a facial recognition system. A facial recognition system creates unique templates stored in an enrolled data base. These data bases are used then to verify a person in a one-to-one match or identify a person in a one-to-many search.

If a match is found, that person is identified with greater or lesser certainty depending on the system in use, the threshold and settings in place, and the operator's expertise. Thus, recognition systems involve matching two images. Without additional processing, they do not impute other characteristics to the person or image.

There's been a great deal of confusion on this point in the media, particularly in contrast to facial characterization or emotion detection software, which attempts to analyze a single image and impute characteristics to that image, including gender and race. These systems may or may not link data to particular individuals, but they carry their own significant risks.

Accuracy requirements and capabilities for recognition and characterization systems vary with context. The level of certainty acceptable for verifying an individual's identity when unlocking a mobile device is below the standard that should be required for verifying that an individual is included on a terrorist watch list.

In addition, quality varies widely among suppliers, based on liveness detection, the diversity of training datasets, and the thoroughness of testing methodologies. The high quality of systems at the top of the NIST rankings reflect their ability to meet these goals. For example, the most recent NIST report highlights accuracy outcomes that were 100 times worse for certain groups, but the best systems achieved results across demographic groups with variations that were, in NIST's words, "undetectable."

However, the real harms arising from inaccurate recognition and characterization systems cannot be ignored. Individuals already use facial recognition to open their phones, access bank accounts, and organize their photos. Organizational benefits include more secure facility access, enhanced hospitality functions, and personalized experiences. New uses are being imagined all the time, but the potential harms are real. In addition to inaccuracy, concerns about real-time surveillance societies have led individuals and policymakers to express significant reservations. The decision by some municipalities to legislatively ban all use of facial recognition systems by government agencies reflects these heightened concerns.

The ethical considerations of where and how to use facial recognition systems exceed traditional privacy considerations, and the regulatory challenges are complex. Even relatively straightforward legal liability questions prove difficult when many parties bear some share of responsibility. When considering the scope of industries hoping to use this technology, from educational and financial institutions to retail establishments, the potential impacts on individuals are mindboggling.

As with many technologies, facial recognition applications offer benefits and generate risks based on context. Tracking online preferences and personalizing consumer experiences are features some people value, but others strongly oppose. Tying these options closely to the appropriate consent level is essential.

While FPF prefers a comprehensive privacy bill to protect all sensitive data, including biometric data, we recognize that Congress may choose to consider technology-specific bills. If so, our facial recognition privacy principles provide a useful model, particularly in requiring the default for commercial identification or verification systems to be opt-in—that is, express affirmative consent prior to enrollment. Exceptions should be few, narrow, and clearly defined, and further restrictions should be tiered and based on the scope and severity of potential harms.

Thank you for your attention and your commitment to finding a responsible regulatory approach to the use of facial recognition technology.

Chairwoman MALONEY. Thank you.

The chair now recognizes Dr. Romine for five minutes.

STATEMENT OF CHARLES ROMINE, PH.D., DIRECTOR, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Mr. ROMINE. Chairwoman Maloney, Ranking Member Jordan, and members of the committee, I'm Chuck Romine, Director of the

Information Technology Laboratory at the Department of Commerce's National Institute of Standards and Technology, known as NIST. Thank you for the opportunity to appear before you today to discuss NIST's role in standards and testing for facial recognition technology.

In the area of biometrics, NIST has been working with public and private sectors since the 1960's. Biometric technologies provide a means to establish or verify the identity of humans, based upon one or more physical or behavioral characteristics. Face recognition technology compares an individual's facial features to available images for verification or identification purposes.

NIST's work improves the accuracy, quality, usability, interoperability, and consistency of identity management systems and ensures that United States interests are represented in the international arena. NIST research has provided state-of-the-art technology benchmarks and guidance to industry and to U.S. Government agencies that depend upon biometrics recognition technologies. NIST's Face Recognition Vendor Testing Program, or FRVT, 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, including the FBI, DHS, CBP, and IARPA.

The NIST FRVT Interagency Report 8280, released in December 2019, quantified the accuracy of face recognition algorithms for demographic groups defined by sex, age, and race or country of birth for both one-to-one and one-to-many identification search algorithms. It found empirical evidence for the existence of demographic differentials in face recognition algorithms that NIST evaluated. The report distinguishes between false-positive and false-negative errors and notes that the impact of errors is application dependent.

NIST conducted tests to quantify demographic differences for 189 face recognition algorithms from 99 developers, using four collections of photographs, with 18.27 million images of 8.49 million people. These images came from operational data bases provided by the State Department, the Department of Homeland Security, and the FBI.

I'll first address one-to-one verification applications. Their false-positive differentials are much larger than those related to false negatives and exist across many of the algorithms tested. False positives might present a security concern to the system owner, as they may allow access to impostors. Other findings are that false positives are higher in women than in men and are higher in the elderly and the young compared to middle-aged adults.

Regarding race, we measured higher false-positive rates in Asian and African American faces relative to those of Caucasians. There are also higher false-positive rates in Native American, American Indian, Alaskan Indian, and Pacific Islanders. These effects apply to most algorithms, including those developed in Europe and the United States.

However, a notable exception was for some algorithms developed in Asian countries. There was no such dramatic difference in false positives in one-to-one matching between Asian and Caucasian faces for algorithms developed in Asia. While the NIST study did not explore the relationship between cause and effect, one possible connection and an area for research is the relationship between an algorithm's performance and the data used to train the algorithm itself.

I'll now comment on one-to-many search algorithms. Again, the impact of errors is application dependent. False positives in one-to-many searches are particularly important because the consequences could include false accusations. For most algorithms, the NIST study measured higher false-positive rates in women, African Americans, and particularly in African American women. However, the study found that some one-to-many algorithms gave similar false-positive rates across these specific demographics. Some of the most accurate algorithms fell into this group.

This last point underscores one overall message of the report. Different algorithms perform differently. Indeed, all of our FRVT reports note wide variations in recognition accuracy across algorithms, and an important result from the demographic study is that demographic effects are smaller with more accurate algorithms.

NIST is proud of the positive impact it has had in the last 60 years on the evolution of biometrics capabilities. With NIST's extensive experience and broad expertise, both in its laboratories and in successful collaborations with the private sector and other 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 on NIST's activities in face recognition and identity management, and I'd be happy to answer any question that you have.

Chairwoman MALONEY. Ms. Whittaker?

STATEMENT OF MEREDITH WHITTAKER, CO-FOUNDER AND CO-DIRECTOR, AI NOW INSTITUTE, NEW YORK UNIVERSITY

Ms. WHITTAKER. Chairwoman Maloney, Ranking Member Jordan, and members of the committee, thank you for inviting me to speak today.

My name is Meredith Whittaker, and I'm the co-founder of the AI Now Institute at New York University. We're the first university research institute dedicated to studying the social implications of artificial intelligence and algorithmic technologies. I also worked at Google for over a decade.

Facial recognition poses serious dangers to our rights, liberties, and values, whether it's used by the state or private actors. The technology does not work as advertised. Research shows what tech companies won't tell you, that facial recognition is often inaccurate, biased, and error-prone. And there's no disclaimer to warn us that the populations already facing societal discrimination bear the brunt of facial recognition's failures.

As Dr. Romine mentioned, the most recent NIST audit confirmed that some systems were 100 times less accurate for black and Asian people than for white people. But this isn't facial recognition's only problem, and ensuring accuracy will not make it safe.

Facial recognition relies on the mass collection of our biometric data. It allows government and private actors to persistently track where we go, what we do, and who we associate with. Over half of Americans are already in a law enforcement facial recognition data base, and businesses are increasingly using it to surveil and control workers and the public. It's replacing time clocks at job sites, keys for housing units, safety systems at schools, security at stadiums, and much more.

We've seen real-life consequences. A facial recognition authentication system used by Uber failed to recognize transgender drivers, locking them out of their accounts and their livelihoods.

Facial recognition and analysis are also being used to make judgments about people's personality, their feelings, and their worth based on the appearance of their face. This set of capabilities raises urgent concerns, especially since the claim that you can automatically detect interior character based on facial expression is not supported by scientific consensus and recalls discredited pseudoscience of the past.

Most facial recognition systems in use are developed by private companies, who license them to governments and businesses. The commercial nature of these systems prevents meaningful oversight and accountability, hiding them behind legal claims of trade secrecy. This means that researchers, lawmakers, and the public struggle to answer critical questions about where, how, and with what consequences this technology is being used. This is especially troubling since facial recognition is usually deployed by those who already have power—say, employers, landlords, or the police—to surveil, control, and in some cases oppress those who don't.

In Brooklyn, tenants in the Atlanta Plaza Towers pushed back against their landlord's plans to replace key entry with facial recognition, raising questions about biometric data collection, racial bias, and the very real possibility that invasive surveillance could be abused by the landlord to harass and evict tenants, many of whom were black and Latinx women and children.

To address the harms of this technology, many have turned to standards for assessment and auditing. These are a wonderful step in the right direction, but they are not enough to ensure that facial recognition is safe. Using narrow or weak standards as deployment criteria risks allowing companies to assert that their technology is safe and fair without accounting for how it will be used or the concerns of the communities who will live with it. If such standards are positioned as the sole check on these systems, they could function to mask harm instead of preventing it.

From aviation to healthcare, it is difficult to think of an industry where we permit companies to treat the public as experimental subjects, deploying untested, unverified, and faulty technology that has been proven to violate civil rights and to amplify bias and discrimination. Facial recognition poses an existential threat to democracy and liberty and fundamentally shifts the balance of power between those using it and the populations on whom it's applied. Congress is abdicating its responsibility if it continues to allow this technology to go unregulated. And as a first step, lawmakers must act rapidly to halt the use of facial recognition in sensitive domains by both government and commercial actors.

If you care about the over-policing of communities of color or gender equity or the constitutional right to due process and free association, then the secretive, unchecked deployment of flawed facial recognition systems is an issue you cannot ignore. Facial recognition is not ready for primetime. Congress has a window to act, and the time is now.

Chairwoman MALONEY. Thank you.

The chair now recognizes Daniel Castro for five minutes.

STATEMENT OF DANIEL CASTRO, VICE PRESIDENT AND DIRECTOR, CENTER FOR DATA INNOVATION, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION

Mr. CASTRO. Thank you. Chairwoman Maloney, Ranking Member Jordan, and members of the committee, thank you for the invitation to testify today.

There are many positive uses of facial recognition technology emerging in the private sector. Airlines are using it to help travelers get through the airports faster, saving people time and hassle. Banks are using it to improve security, helping reduce financial fraud. Hospitals are using it to verify the right patient receives the right treatment, preventing medical errors. There is even an app that says it uses facial recognition on dogs and cats to help find lost pets.

Americans are increasingly familiar with commercial uses of the technology because it's now a standard feature on the latest mobile phones. It's also being integrated into household products like security cameras and door locks. There is one—this is one reason why a survey last year found the majority of Americans disagreed with strictly limiting the use of facial recognition if it would mean airports can't use the technology to speed up security lines. And nearly half opposed strict limits if it would prevent the technology being used to stop shoplifting.

But over the past year, I've also seen headlines suggesting that facial recognition technology is inaccurate, inequitable, and invasive. If that was true, I would be worried, too, but it isn't. Here are the facts.

First, there are many different facial recognition systems on the market. Some perform much better than others, including in their accuracy rates across race, gender, and age. Notably, the most accurate algorithms NIST has evaluated show little to no bias. These systems continue to get measurably better every year, and they can outperform the average human.

Second, many of the leading companies and industries responsible for developing and deploying facial recognition have voluntarily adopted robust privacy and transparency guidelines. These include voluntary standards for digital signs and consensus-based, multi-stakeholder guidelines developed for the broader technology community.

But while the private sector has made significant progress on its own, Congress also has an important role. I'd like to suggest seven key steps.

First, Congress should pass comprehensive legislation to streamline consumer privacy regulation, preempt state laws, and establish basic data rights. While it may be appropriate to require opt-in consent for certain sensitive uses, such as in healthcare or education, it won't always be feasible. For example, you probably can't get sex offenders to agree to enroll in it. So, opt-ins should not be required across the board.

Legislation should also be technology neutral, and it shouldn't treat facial recognition differently than other types of biometrics. In addition, a Federal law should not establish a private right of action because that would significantly raise costs for businesses, and these costs would eventually be passed on to consumers.

Second, Congress should direct NIST to expand its evaluation of commercial facial recognition systems to reflect more real-world commercial uses, including cloud-based systems and infrared systems. NIST also should continue to report performance metrics on race, gender, and age, and NIST should develop a diverse facial images dataset for training and evaluation purposes.

Third, Congress should direct GSA to develop performance standards for any facial recognition system that the Government procures, including for accuracy and error rates. This will ensure Federal agencies don't waste tax dollars on ineffective systems or systems with significant performance disparities.

Fourth, Congress should fund deployments of facial recognition systems in Government. For example, using it to improve security in Federal buildings and expedite entry for Government workers.

Fifth, Congress should continue to support Federal funding for research to improve the accuracy of facial recognition technology as part of the Government's overall commitment to investing in artificial intelligence. One of the key areas of fundamental AI research is computer vision, and the U.S. Government should continue to invest in this technology, especially as China makes gains in this field.

Sixth, Congress should consider legislation to establish a warrant requirement for authorities to track people's movements, including when they use geolocation data from facial recognition systems.

Finally, Congress should continue providing due oversight of law enforcement. That should include ensuring that any police surveillance of political protests is justified and conducted with appropriate safeguards, and it should include scrutinizing racial disparities in the use of force among communities of color.

Congress also should require the Department of Justice to develop best practices for how state and local authorities use facial recognition. This guidance should include recommendations on how to publicly disclose when law enforcement will use the technology, what sources of images will be used, and what the data retention policies will be.

Congress should always consider the impact of new technologies and ensure there are proper guardrails in place to protect society's best interests. In the case of facial recognition technology, there are many unambiguously beneficial opportunities to use the technology, such as allowing people who are blind or who suffer from face blindness to identify others. So, rather than imposing bans or moratoriums, Congress should support positive uses of the technology while limiting the potential misuse and abuse.

Thank you again. I look forward to answering any questions.

Chairwoman MALONEY. Thank you.

Jake Parker is recognized for five minutes.

STATEMENT OF JAKE PARKER, SENIOR DIRECTOR OF GOVERNMENT RELATIONS, SECURITY INDUSTRY ASSOCIATION

Mr. PARKER. Good morning, Chairwoman Maloney, Ranking Member Jordan, and distinguished members of the committee.

My name is Jake Parker, Director of Government Relations for the Security Industry Association. SIA is a trade association representing businesses that provide a broad range of security products for the Government, commercial, and residential users while employing thousands of innovators in the United States and around the globe.

Our members include many of the leading developers of facial recognition technology and many others that offer products that incorporate or integrate with this technology for a wide variety of applications. SIA members are developing tools and technologies to enhance security and convenience for consumers and enterprise users.

It is because of the experience our members have in building and deploying this technology, we are pleased to be here today to talk to you about how it can be used consistent with our values. We firmly believe that all technology products, including facial recognition, should only be used for lawful, ethical, and nondiscriminatory purposes. That way, we as a society can have confidence that facial recognition makes our country safer and brings value to our everyday lives.

So, in commercial settings, facial recognition offers tremendous benefits. For example, it could be used to allow individuals to securely, quickly, and conveniently prove their identity in order to enter a venue, board a commercial airplane, perform online transactions, or seamlessly access personalized experiences. In addition, companies are using the technology to improve the physical security of their property and their employees against the threat of violence, theft, or other harm.

Additionally, as you know, Government agencies have made effective use of facial recognition for over a decade to improve homeland security, public safety, and criminal investigations. And one important example of the use of this technology is to identify and rescue trafficking victims. It's been used almost—in almost 40,000 cases in North America, identifying 9,000 missing children and over 10,000 traffickers.

According to news reports, a law enforcement officer in California last year saw a social media post about a missing child from the National Center for Missing and Exploited Children. After law enforcement used facial recognition, the victimized child was located and recovered.

In another notable success story, NYPD detectives last year used this technology to identify a man who sparked terror by leaving a pair of rice cookers at the Fulton Street Subway. Using facial recognition technology, along with human review, detectives were able to identify the suspect within an hour. The chief of detectives was quoted as saying, "To not use this technology would be negligent."

Both public and private sectors have seen that better cameras, better devices with more computing power, combined with more effective software, can provide security-enhancing tools. From unlocking mobile phones to securing critical infrastructure, facial recognition technologies abound.

But in all applications, SIA members see transparency as the foundation that governs the use of facial recognition technology. It should be clear when and under what circumstances the technology is used, as well as the processes governing the collection, processing, and storage of related data.

We support sensible safeguards that promote transparency and accountability as the most effective way to ensure the responsible use of the technology without unreasonably restricting tools that have become essential to public safety. Additionally, SIA does not support moratoriums or blanket bans on the use of this important technology.

As the committee works on the proposals mentioned earlier requiring greater accountability for Federal Government use, we encourage private sector developers to be brought into the conversation to present our real-world views on how the technology works and should be best managed. We hope you also remember the important role the Government plays in supporting biometric technology improvements. At a minimum, Congress should provide NIST with the resources it needs to support the expansion of these efforts.

As we think about regulation, we believe that any effort specific to commercial use makes sense in the context of the National Data Privacy Policy. Many legislative efforts in this area include biometric information, and was said earlier, we think this needs to be tech neutral. This is the right approach to include.

In the meantime, we encourage our members to play an active role in providing end-users with the tools they need to use this technology responsibly. In order to make this come to fruition, SIA is developing a set of use principles on the technology.

As this hearing comes on the heels of a recent NIST study, which generated a lot of news and a fair amount of controversy, it's important to note that biometric technology companies have been working closely with NIST for decades, handing over their technology and allowing the Government to rigorously test it and publicly post the results. And it's improving every year to the point where the accuracy is reaching that of automated fingerprint comparison, which is viewed as the gold standard for identification.

The most important, significant takeaway from the NIST report is that it confirms facial recognition technology performs far better across racial groups than had been widely reported before. According to NIST data, only four out of 116 verification algorithms tested using the mug shot data base had false match rates more than 1 percent for any demographic. While that's tremendous progress for users of biometrics, we are committed to continuing to provide technology so that all users can be comfortable with it in the transparency and privacy policy surrounding its deployment to improve the technology.

On behalf of SIA, thanks for the opportunity to appear before you today, and we look forward to working with you.

Chairwoman MALONEY. Thank you.

Dr. Romine, I would like to ask you about the study that you released last month and that you mentioned in your testimony. And

I would like to ask unanimous consent to place that study in the record, without objection.

Chairwoman MALONEY. We all know that commercial facial recognition technology continues to expand in both the public and private sectors, but your new study found that facial recognition software misidentified persons of color, women, children, and elderly individuals at a much higher rate. And in your study, you evaluated 189 algorithms from 99 developers. Your analysis found that false positives were more likely to occur with people of color, and is that correct?

Mr. ROMINE. It is correct for the largest collection of the algorithms. That's correct.

Chairwoman MALONEY. And your report also found that women, elderly individuals, and children were more likely to be misidentified by the algorithms. Is that correct?

Mr. ROMINE. That is correct for most algorithms.

Chairwoman MALONEY. Now in women's health, they used to do all the studies on men. When you were doing these studies, were you doing them on men's faces as a pattern, or were you using women's faces?

Mr. ROMINE. No, we had a substantial set of images that we could pull from, and so we were able to represent a broad cross-section of demographics.

Chairwoman MALONEY. OK. Did these disparities and false positives occur broadly across the algorithms that you tested?

Mr. ROMINE. They did occur broadly for most of the algorithms that we tested.

Chairwoman MALONEY. And your study states, and I quote, "Across demographics, false-positive rates often vary by factors or 10 to beyond 100 times." These are staggering numbers, wouldn't you say? How much higher was the error rate when the algorithms were used to identify persons of color as compared to white individuals?

Mr. ROMINE. So, as we state in the report, the error rates for some of the algorithms can be significantly higher, from 10 to 100 times the error rates of identification for Caucasian faces for a subset of the algorithms.

Chairwoman MALONEY. And what was the difference in the misidentification rate for women?

Mr. ROMINE. Similar rates of——

Chairwoman MALONEY. Ten to 100?

Mr. ROMINE. Ten to 100. I'll have to get back to you on the exact number, but it's certainly a substantial difference on some algorithms.

Chairwoman MALONEY. What about black women? Is that higher?

Mr. ROMINE. Black women have a higher rate of—on some algorithms, on the same algorithms that we're discussing, than either black faces broadly speaking or women broadly speaking. Black women were even—had differentials that were even higher than either of those two other demographics.

Chairwoman MALONEY. So, what were they?

Mr. ROMINE. Substantially higher. On the order of 10 to 100.

Chairwoman MALONEY. OK. And misidentification, as we all know, can have very serious consequences for people when they are falsely identified. It can prevent them from boarding a plane or entering the country. It can lead to someone being falsely accused or detained or even jailed.

So, I am deeply concerned that facial recognition technologies have demonstrated racial, gender, and age bias. Facial recognition technology has benefits to be sure, but we should not rush to deploy it until we understand the potential risks and mitigate them. Your study provides us with valuable insight into the current limitations of this technology, and I appreciate the work that you have done and all of your colleagues on the panel today that have increased our understanding.

I would now recognize the ranking member. No? I am going to recognize the gentlelady from North Carolina, Ms. Foxx. She is now recognized for questions.

Ms. FOXX. Thank you, Madam Chairman.

Mr. Parker, how competitive is the facial recognition technology market?

Mr. PARKER. It's extremely competitive because of the advances in technology over the last couple years. Particularly the dramatic increase in accuracy in the last three to five years combined with advances in imaging technology have really made the products more affordable, and therefore, there's been more interest from consumers and then more entry to the market from competitors.

Ms. FOXX. To what extent do the companies compete on accuracy, and how could a consumer know more about the accuracy rates of the facial recognition?

Mr. PARKER. OK. So, they do compete on accuracy, and you know, the NIST program plays a really helpful role here in providing a useful benchmark in measurement of accuracy. And so the companies are competing to get the best scores on those tests. Companies also do their own private testing and make those results available to their customers.

And there is an important distinction, though, as well because in the NIST testing, you have static data sensors, specific photo sets they are using that are already there, whereas those aren't necessarily the same type of images that you'd be seeing in a deployed system. And so other types of tests need to be done of a fully deployed system to really determine what its accuracy is.

Ms. FOXX. What private sector best practices exist for securing facial images and the associated data, such as face print templates and match results, in these facial recognition technology systems?

Mr. PARKER. So, as I mentioned earlier, SIA is developing a set of best use practices, but that's based on the fact that many of our members have produced best practices they work with their customers on to implement that would accomplish privacy goals. I have a couple of examples, but one of the most significant things to mention here is that many of these products already have built into them the ability to comply with data privacy laws in Europe, so the GDPR laws in Europe. And so this has to do with encrypting photos, encrypting any kind of personal information that's associated with it, securing channels of communication between the server and the device, as well as procedures for looking up someone's information, being able to delete that if requested, and being able to tell someone what information is in the system.

Ms. FOXX. Could you summarize succinctly some of the best practices that exist for protecting that personally identifiable information that is incorporated into it? Is it too complicated a system to explain here? Is there something we could have to read or——

Mr. PARKER. Sure. I'd be happy to provide some more details later, but certainly one of the most important things is encryption of the data. So, that prevents its usefulness if it there is a data breach. Also, it's important to point out that the—we talked about the face template is what the system uses to make a comparison between two photos. So, by itself, that's basically like the digital version of your fingerprint is turned into a number in the fingerprint system. By itself, if that data is compromised, it's not useful to anyone because the proprietary software is the only thing that can read it.

Ms. FOXX. I have been reading a lot about the difference between Europe and us in developing these kinds of techniques recently. A number of state and international policies are impacting how information is collected. For example, Illinois, Washington, Europe's GDPR directly address privacy information. How have commercial entities conformed to these new legal structures?

Mr. PARKER. So, what we're seeing is that we're adapting here and that we're already building in these features to products in anticipation, first of all, because it's just good practices, right, many of the things the GDPR requires. But also, we anticipate there to be a similar framework here at this country at some point, and so being proactive in building some of those things in.

Ms. FOXX. Thank you, Madam Chairman. I yield back.

Chairwoman MALONEY. We now recognize the gentlewoman from the District of Columbia. Ms. Norton is now recognized for questions.

Ms. NORTON. Thank you, Madam Chair.

This is an important hearing, but I must say I think we are playing catch-up. And the way to demonstrate that, I think, most readily is what the cell phone companies are already doing with this technology. Private industry appears to be way ahead of where the Congress or the Federal Government is, and the interesting thing is they are responding to consumers.

And it appears that consumers may already be embracing facial recognition in their own devices because the latest—as they compete with one another, almost all of them have incorporated facial recognition already in their latest mobile products. And of course, if one does it, the other is going to do it. And Apple and Samsung and all the rest of them already do it.

You can unlock your cell phone by scanning your face. Now the public thinks this is, and I suppose they are right, this is a real convenience instead of having to log in those numbers. And they have grown accustomed, frankly, to cameras. I remember when cameras were first introduced in the streets, and people said, oh, that is terrible. Then, of course, there is no right to privacy once you go in the streets. But talking about my cell phone, there is a lot of private information in there.

And according to recent reports, this technology is not foolproof. That is my concern. That, for example, a simple photograph can fool it in some instances or unauthorized individuals could get into your cell phone, and any sensitive information that you happen to have in there, and a lot of people store things like, of course, their email is there, but banking and the rest of it.

Ms. Leong, do you see problems that are already there of companies now integrating facial technology onto consumer devices like this, and are we too far behind to do anything about it? Because it looks like the public sees convenience, and I don't hear anybody protesting it. Would you comment?

Ms. LEONG. Thank you very much.

I think that's an excellent question, since we do see the use cases advancing quickly in many applications, as you say, with phones being one of the most personalized ones that people have. I think they make a good example, too, of some of the variations that are in place in the market of the different ways that facial recognition technology is being used.

For example, in your phone, I'm going to use Apple as the example, and this is my best understanding. I obviously don't work for or speak for Apple. Takes a representative picture of your face, using both infrared technology and 3-D imaging in order to prevent things like using a photo or using another person. And it takes at a level of detail that stands up to about a 1 in 10 million error rate, which is a pretty substantive level for something that is, in fact, part of a two-factor process. You have to have the phone, and then you have to know whose phone it is and have their face, and then you have to match whatever that standard is. So, that's actually a pretty robust standard for the level of risk involved in what might be—you know, have a lot of personal data but is one level of concern for people being violated.

A facial recognition system that identifies somebody off of a video feed as a suspect in a crime would be an entirely different level of risk, entirely different level of implication on that person, and certainly should be considered and potentially regulated in a very different way than that. So, yes, I do think we see those things being used in different ways already. Some of those have already started to have some blowback on them in things like the criminal justice system, and that, I think, is what has really gotten people's attention and said where are the places that we need to draw those lines and say it shouldn't be used here in these cases maybe at all, or if it is, it should be used in very limited and regulated ways.

Ms. NORTON. Ms. Whittaker, can I ask you about the average consumer? Does the average consumer have any way to confirm—should they have any way to confirm that these cell phone manufacturers are, in fact, storing their biometric or other data on their servers? What should we do about that? Consumer knowledge?

Ms. WHITTAKER. Yes, the average consumer does not, and indeed, many researchers, many lawmakers don't because this technology, as I wrote about in my written testimony, is hidden behind trade secrecy. This is a corporate technology that is not open for scrutiny and auditing by external experts.

I think it's notable that while NIST reviewed 189 algorithms for their latest report, Amazon refused to submit their recognition algorithm to NIST. Now they claimed they couldn't modify it to meet NIST's standards, but they are a multibillion-dollar company and have managed some other pretty incredible feats. So, whatever the reason is, what we see here is that it's at the facial recognition company's discretion what they do or don't release. That they release accuracy numbers oftentimes that aren't validated or that it's not possible to validate by the general public. So, we're left in a position where we have to trust these companies, but we don't have many options to say no or to scrutinize the claims they make.

Ms. NORTON. Thank you, Madam Chair.

Chairwoman MALONEY. Thank you.

The gentleman from Louisiana, Mr. Higgins, is now recognized for questions.

Mr. HIGGINS. Thank you, Madam Chair.

I would like to ask unanimous consent that the statement of Chief James Craig, the Detroit Police Department, his written testimony be entered into the record. The chief has had a tremendous amount of success using facial recognition technology.

Chairwoman MALONEY. Without objection.

Mr. HIGGINS. Thank you.

And I would also like to recognize and thank our esteemed colleague Representative Gomez for his opening statement. Standing upon principles of freedoms and liberties, protecting freedoms and liberties, and resisting and curtailing the manifestation of Big Brother, reducing and controlling the size and scope of Federal powers. And I want you to know, good sir, the Republican Party welcomes your transition.

[Laughter.]

Mr. HIGGINS. Madam Speaker, facial recognition technology is an emerging technology, and of course, it is produced by private entities. Law enforcement doesn't produce its own technologies. It is coming, and it is here. It will get better as the weeks and months move forward. It should be no surprise to us that the effective percentages of identification using a new technology will increase as time moves forward.

And there is more coming. There is total person recognition technology coming that measures the specific physical features of individuals, their gait, length of their arms, et cetera. This technology is coming. Now what we should seek is a means by which to make sure that Big Brother is not coming.

I have a background in law enforcement, and recognition technology has become manifest in many ways. You have license plate readers being used from sea to shining sea. These are readers in police units that drive around and read license plates. If we are looking for a suspect vehicle and, you know, we have an eye out for a particular vehicle, a particular color, that is human recognition. We see that vehicle. We read the license plate. We have license plate readers reading every plate we pass.

If it is expired or the associated driver's license to that registered vehicle is a person that is wanted, then we will keep an eye on that vehicle. And if the guy that walks out the building and gets in that vehicle appears to be the suspect that we have identified or we have a warrant for, then there is going to be some interaction there. This is a technology that has evolved and become manifest over the last 15 or 20 years. It has gotten very effective.

Prior to facial recognition technology, it was completely common that we used digital record from crime scene, images frozen, the best picture we could get from a crime scene video, from surveillance cameras at the business, or whatever was available to us. We would pass these images on, have the shifts watch these images. And someone at shift, the odds are pretty good somebody would recognize that guy. But this is the beginning. Recognition is the beginning of an investigation. It helps law enforcement cultivate a person of interest for us to speak to.

There can never be a time where—there are just two things we stand against, and this is where the ranking member and I have had discussions at length. Both of us stand against live streaming the images of free Americans as they travel and enter businesses or go to-and-fro across America through some data base where, all of a sudden, the police show up to interview that guy. But solving a crime, we are already using digital images to the best of our ability to solve crimes, and every American should recognize that this is an important tool.

The chief's written statement, which I have asked to be submitted and the chairwoman has graciously accepted, has several examples of incredible success using this technology. Now I am going to have a question I will submit in writing, if I may, Madam Chair, for Mr. Parker and Mr. Romine and Ms. Whittaker. I have three specific questions, which time will not allow.

This is an important topic. We have had several hearings about it. I thank the majority party's focus on this, and I hope that we can come together with effective legislation that both allows the technology to move forward as a law enforcement tool and protects the freedoms and privacy of the American citizens we serve.

I yield.

Chairwoman MALONEY. Thank you.

I now recognize the gentleman from Massachusetts. Mr. Lynch is now recognized for questions.

Mr. LYNCH. Thank you very much, Madam Chair. And I want to thank you and the ranking member for collaborating on this hearing and approaching it in the right way, I think.

First of all, I want to thank the witnesses for your testimony. I think it is very helpful. As I understand it, and I am not sure—I am a little skeptical—they tell me that the facial recognition that you use on your phone with the iPhone that at least the way iPhone says they handle this is that the indicia of identity stays on the phone and doesn't go up to a server at this point. But, you know, I sort of question whether they will have that ability to do that in the future.

I think there is probably a greater danger that they will get facial recognition right. You know, it is not the misses that I am concerned about right now, although that has to stop. It is what happens when they have all this data out there, whether it is law enforcement or private firms.

We had a massive data breach by Suprema, which is a big biometrics collector, 100 million people, I think. No, I am sorry, 27 million people in that breach. And then Customs and Border Patrol, 100,000 people that they identified, along with license plates, that was breached. So, the concern is once this information is collected, it is not secure. And that is a major problem for all of us.

I want to ask some specific questions about TikTok. So, TikTok is a Chinese company—well, it was purchased by a Chinese company. It is a musical video app that the kids love, I think. They tell me that in the last 90 days a billion people have downloaded it in the U.S. and in Europe, and it is owned by the Chinese government.

And—I am sorry. It is located in Beijing, and under Chinese law, the recent national security law in China, they have to cooperate, they have to cooperate with the Chinese government. And we already see it happening. If you look on TikTok, you don't see much about the protests in Hong Kong. They are already exercising censorship on TikTok.

So, TikTok would have to cooperate with China. So, that is a national security concern for us. CFIUS is looking at it. It is under review.

The other situation is Apple phone, the iPhone and our efforts, because of the Pensacola shootings, we are trying to get Apple to open up the iPhone so we can get that information. If you step back, it is sort of what we are worried about China doing, what we are doing with Apple. We are trying to get access to that data, just like China can get all that data from TikTok.

How do we resolve that dilemma? Is there a way, Dr. Romine, that we can protect our citizens and others who share that data or have their identity captured, you know, their facial recognition captured? How do we resolve that so that we use it to the benefit of society?

Mr. ROMINE. Thank you for the question.

I think the bottom line really is balancing the understanding of the risks associated with policy decisions that are made. Those policy decisions are outside of NIST's purview, but with regard to the debate on, you know, access to Apple and encryption, we know that in the Government and broadly speaking, there are two——

Mr. LYNCH. OK. If it is not in your discipline, let me ask Ms. Whittaker. Same question.

Ms. WHITTAKER. Thank you for the question.

I think that the short answer there is that we don't have the answer to that question. We have not done the research that is needed to affirmatively answer that, yes, we can protect people's privacy, their liberty when these technologies are deployed at wide scale in a complex geopolitical context. I think we need more of that research, and we need clear regulations that ensure that these are safe.

Mr. LYNCH. All right. Mr. Castro, anything to add?

Mr. CASTRO. Yes, I'd just say, I mean, I think we need to unabashedly support encryption. I think when, you know, you have end-to-end encryption, consumers have control over the data, and then the third parties don't. If we back that, that's the way you give consumers control of the information. That's how you keep out the hand of government on either side.

Mr. LYNCH. All right. I have exhausted my time. Madam Chair, thank you for your courtesy. I yield back.

Chairwoman MALONEY. Thank you so much.

The gentleman from Texas, Mr. Cloud, is now recognized for questions.

Mr. CLOUD. Hello. Thank you all again for being here and your work on this topic. This is an extremely important topic that, obviously, we are going through the birth pains of development on this new technology.

Mr. Parker, the Government use of facial recognition technology, are they using technologies that are primarily developed by the Government or commercial entities?

Mr. PARKER. I believe that's a mixture of both. So, in some cases, especially with Federal agencies, they have developed their own systems over time, but I think increasingly it's moving to commercial solutions, I believe.

Mr. CLOUD. Commercial solutions. And Dr. Romine—maybe, Mr. Castro, you can help with this—what has been the industry response to the NIST report?

Mr. ROMINE. From our perspective, industry has been involved from the outset. They've been very supportive of the efforts that we've undertaken in FRVT over the last 20 years. So, it's been a—it's generally a very positive thing. Industry feels challenged to do better.

Mr. PARKER. I can just add I think it depends on the industry. You know, those that are participating really value it, but as I noted, I mean, it's excluding a lot of the technologies that we're using today. So, it excludes, for example, Amazon because Amazon is a cloud-based system. It excludes Apple's because Apple's is an infrared system. We need to include those as well.

Mr. CLOUD. OK. And Mr. Castro and Mr. Parker, you both mentioned that it has been improving dramatically year by year, I guess. Would you say that we are weeks, months, years, decades away from getting this technology to an acceptable——

Mr. CASTRO. I think if you look at the best-performing algorithms right now, they are at that level of acceptance that we would want. There are, you know, error rates of 0.01 percent. I mean, that's incredibly small. And so when we're talking about even the magnitude of difference between error rates, if you have something that's 10 times worse, that's still 0.1 percent error rate. And it's 0.1 percent error rate. So, that's, you know, 1 out of 10,000; 1 out of 1,000. These are very small numbers.

Mr. CLOUD. All right. Mr. Parker?

Mr. PARKER. Yes, so we're reaching, right—as Mr. Castro said, we're reaching that point now. I think, you know, so there are some reasons why the industry is really focused on the false-negative type error rates and reducing that over time. And I think what—and that's down to extremely low levels now. And this is documented that it's 20 times better now than it was five years ago.

But I think given the results of the demographic effect study, we are looking at now some of the false-positive rates in trying to make those more uniform. So, you know, the way that, you know, achieving homogenous rates, the way NIST defined that is those that are mostly the same across different demographic groups.

And so, I think, there is important context to consider these in. One is, that has been mentioned already, the total relative scale.

I mean 100 times 0.01 is 1 percent. But also, it's the context of what the consequences of errors could be, and in some cases, it matters more than others.

So, like with law enforcement investigations, NIST actually says in its report, the false-positive differentials from the algorithm are immaterial. And the reason why that is, is because the way law enforcement uses the technology, they're looking at a set number of potential candidates that meet a criteria, usually like 50.

In the case of a New York City incident I mentioned before, they actually looked through hundreds of photos that were potential matches. So, there is that human element there. The technology functions as a tool to enhance their job. It's still up to a human to decide whether there is an actual match. So, in that case, the false-negative error effect is much more important because you want to make sure that you're not missing someone that's actually in your dataset.

Mr. CLOUD. Yes. Could you speak potentially to the—how do we get this right from our perspective of where we sit? Because sometimes, you know, in advancements in technology or anything else, sometimes we step in as the Federal Government to fix a problem and actually end up creating an environment that prohibits the technological advancements or the natural market things that work to make us get to that solution. Sometimes we actually make us take a step back. So, what is the right approach here?

Mr. PARKER. So, I think, and this relates to what Mr.—Congressman Higgins said earlier, facial recognition is just one of many advanced technologies. It's important that, you know, I think the issues that we have in talking about this are not really—don't really have to do with the technology, they have to do with how it's used.

So, I think we need to focus on addressing the concerns we have through narrowly tailored restrictions, if warranted. And I think that's the more sensible approach, and I think we've actually seen a proposal in the Senate that would do something like that.

Mr. CLOUD. Thank you. I yield back.

Chairwoman MALONEY. I now recognize the gentlewoman from Illinois, Ms. Kelly, for questions.

Ms. KELLY. Thank you, Madam Chair and Ranking Member, for holding this hearing and continuing to make this an important issue for our committee.

We have talked previously about bias in facial recognition and artificial intelligence generally, but the recent NIST Face Recognition Vendor Test Part 3 on Demographic Effects provides useful data on the development of commercial facial recognition programs. As chair of the Tech Accountability Caucus, I have raised concerns about biased and unfair algorithms and the dangers of allowing these biases to perpetuate. The results of the Part 3 report were not particularly surprising, as has been discussed, with women and individuals of African and Asian descent having higher false-positive rates than middle-aged Caucasian men.

Director Romine, in your testimony, I was hoping you could clarify the statement that policymakers and the public should not think of facial recognition as either always accurate or always error-prone. In my opinion, as policymakers, we should be pushing to have these technologies get as close to always accurate as possible. Why should we not strive to think of this technology as always accurate, and how long will we have to wait for this technology to reach close to always accurate for all demographic groups?

Mr. ROMINE. Thank you for the question.

I don't know how long it will be. I can't predict the future. The statement refers to the fact that the characteristics you have to include in any discussion are you have to know the algorithm that you are using. And as my testimony stated, while many of the algorithms that we tested exhibit substantial bias or substantial demographic effects across three different demographics, the most accurate ones do not in the one-to-many categories. So, you have to know the algorithm that you're using.

You also have to know the context. So, the ability to automatically identify Aunt Muriel in a family photo doesn't have a very high risk if you get that wrong. And so I think compare that to, you know, the identification of a suspect, where there are some very serious concerns about ensuring that you get that right. So, those—you have to know the context in which you're using the algorithm. You have to know the algorithm that you're using. And then you have to know the overall system.

We test mathematical algorithms at NIST. We don't have the capacity and we don't test systems that are deployed in the field. And those have implications as well.

Ms. KELLY. While I have you, can you discuss the benefits of auditing facial recognition systems for bias?

Mr. ROMINE. From our perspective, whether it's policymakers or Government entities or private sector entities that want to use face recognition, the most important thing to do is to understand—to have the accurate data—accurate, unbiased data that we can provide, so that appropriate decisions are made with regard to whether to regulate or not, what kinds of regulations might be needed, in what context. If you are in a procurement situation, procuring a system, you want to know the performance of that system and the algorithms that it depends on.

So, those are the things that we think are appropriate. From an auditing capability or an auditing perspective, we don't view the testing that we do as an audit, so much as providing policymakers and Government and the private sector with actionable information.

Ms. KELLY. Ms. Whittaker, I know you talked a little bit about auditing. I would like you to answer, as well as Ms. Leong.

Ms. WHITTAKER. Absolutely. I think auditing is absolutely important, but we need to understand how we're measuring these systems. In my written testimony, I gave an example of one of the most famous facial recognition measurement systems. It was a dataset that we measure these systems against, and it's called Labeled Faces in the Wild. And in short, it features photos of mainly men and mainly white people. So, the way that the industry assessed accuracy was to be able to recognize white men, and that gives us a sense of why we're seeing these pervasive racial and demographic biases across these systems.

So, the standards we choose to measure ourselves by matter greatly. And if those standards don't ask questions about what the data that will be used in these systems in a deployment environment will be, how these systems will be used. If they don't ask questions like what the Atlanta Plaza tenants were concerned about, will they be abused? Will they be used to——

Ms. KELLY. I just want to give Ms. Leong a chance before my time runs out.

Ms. WHITTAKER. OK.

Ms. LEONG. I agree absolutely that the auditing function is critical, and as Ms. Whittaker said, the standards being used both during development and testing and by the companies afterwards matter. One of the regulatory options is to have requirements that say Government use or purchase of systems have to be NIST evaluated or have to be, have been ranked by some external objective tester that has clear transparency into what the standards were and how it was measured and what was done.

Ms. KELLY. Thank you. I yield back.

Chairwoman MALONEY. From the great state of Georgia, Mr. Hice is now recognized for questions.

Mr. HICE. Thank you, Madam Chair.

There is no question this technology of facial recognition is extremely important and viable for our Government, I think, most notably, places like border patrol and law enforcement. At the same time, there is also no question that this technology allows for any individual to be identified in public spaces, be it through private sector or Government entities, and therein lies a potential problem and grave concern for many people. Both, whether we are dealing in private sector or Government, should bear the responsibility of individual privacy and data security.

And so, I am not sure exactly where this question is best directed, be it Mr. Parker, Mr. Castro, Ms. Leong. I am not sure, so any of you jump in here. Are there—let's start with the private sector companies that are using facial recognition technology that are addressing this issue of civil liberty or the whole question of privacy. In other words, are there any within the private sector who are setting forth best practices, any of the stakeholders?

Mr. CASTRO. I can start with that. Yes, we have identified a number of companies that have put out principles around privacy. Specifically, I can name some—Bank One, Microsoft, Amazon, Google. They all have public statements where they identify what specifically they are doing around facial recognition, how they want to protect privacy, how they're doing in terms of development of the technology, what they're doing with developer agreements. So, if anyone is using their technology, what they have to agree to, to use their technology.

Mr. HICE. Like what are some of those principles? What are the guidelines?

Mr. CASTRO. So, it has things around transparency, consent, data protection, notification. They go through a whole set of issues. And these match the type of consensus-based guidelines that we've seen come out of other forums as well.

Mr. HICE. All right. So, we have a big concern, you just brought it up, that people are being identified without their consent. So, how—what are the safeguards? I mean, it is one thing to have policies, to have things written down. It is another thing to implement these things to protect the public, protect individuals who are not—have not consented to this type of technology. So, how will these facial recognition products, as they develop, inform individuals that they are being exposed, potentially without their knowledge?

Mr. CASTRO. So, a number of the recommendations are around how you actually communicate with individuals, under what circumstances. And part of the source of confusion, I think, in some areas is that there's many different types of systems that are out there. So, some are just doing facial analysis. For example, in the digital signage industry, if you walk by an advertising sign——

Mr. HICE. Without consent?

Mr. CASTRO. Without consent. What they're doing is they're just tracking the general demographics of who has seen the ad. They're not tracking anyone's identity.

And so they've said for that type of purpose, they're not going to be doing—they're not going to be obtaining consent. But they have said if they're going to be targeting people ads, so for example, if they're targeting you based on your identity, they will require consent. So, you have to have signed up, for example, for the——

Mr. HICE. All right. So, let's go to the Atlanta airport, which right now is a pilot airport for some facial recognition technology. All right. You have the busiest airport in the world. You have thousands of people walking around all over the place. When this technology is implemented, there is no way to get consent from everyone walking around.

Mr. CASTRO. So, for the Atlanta airport specifically, they have the ability to opt out. So, you don't have to go through that if you are going through the terminal, the international terminal.

Mr. HICE. All right. So, how does a person opt out?

Mr. CASTRO. You simply say that you don't want to use the self-serve kiosk, and you can go to an agent and show them your passport.

Mr. HICE. So, you are saying that technology in airports would be used just in security lines?

Mr. CASTRO. No, it's used for boarding and for screening and for bag check. It's used for a variety of purposes. In each of those areas, Delta has said that they have an ability to opt out, and they allow consumers to do that.

Mr. HICE. OK. Do you know of any case where the Government in particular, using this type of technology without the knowledge, without the consent of an individual, where it actually violated the Fourth Amendment?

Mr. CASTRO. I don't know that. I don't think we have good documentation of that. I do think that's why we need a search warrant requirement, so we know whenever those requests are made.

Mr. HICE. Yes, I would agree. And therein lies the great potential problem with all this. I mean, we see the value of the technology, but somehow we have got to land the plane on a safe zone that does not violate people's rights. And I appreciate you being here.

Thank you, Madam Chair.

Chairwoman MALONEY. Thank you.

The gentlelady from Michigan, Mrs. Lawrence, is now recognized for questions.

Mrs. LAWRENCE. Thank you so much, Madam Chair.

This year, I introduced H.R. 153 with my colleague Representative Khanna, regarding the need for the development of guidelines for the ethical development of AI. Transparency of AI systems, processes, and what implications are a result of it in helping to empower women and underrepresented or marginalized populations. Right now, we have the wild, wild west when it comes to AI. Artificial intelligence isn't the only emerging technology that requires the development of ethical guidelines. The same discussion must be carried over to the use of facial recognition.

There was a member who introduced a statement from the Detroit Police Department. So, I represent a majority minority district, and the city of Detroit is one of my cities. And approximately 67 percent of my constituents are minorities, meaning the vast majority of my constituents have a higher likelihood of being misidentified by a system that was intended to increase security and reduce crime.

Last month, NIST released a study, the Facial Recognition Vendor Test Part 3, which evaluated facial recognition algorithms provided by the industry to develop the accuracy of demographic groups. The report yielded there are higher rates of inaccuracies for minorities to Caucasians. Ms. Whittaker, you stated that if we develop—when algorithms are developed and you do use a biased process, it is going to give you a biased result. And one of the things with the—and we asked the question initially, what can we do?

First of all, there should not be any American citizen who is under surveillance, where it is not required that it is posted and identified in a place to contact that company to say, "What are you using my image for?" We in America have the right to know if we are under surveillance, and what are you doing with it.

Another thing, any release of data that you are gathering should be required to go through some type of process for the release of that. So, I can't just put a camera up, gather information, and then sell it. We are having this conversation about the Ring doorbell. We know that that is helping to get criminals, but if you are going to give the information from Ring to the local police department, there should be some formal process of disclosure and inclusion to the public so that they know that is happening.

I am very concerned about the movement of this technology. So, some places have just said we are not going to use it. And we know this technology is here and is moving forward. Instead of just saying don't use it, we need to be, as Congress, very proactive of setting ethical standards. Have an expectation that our public can say that if I am being—if my image is being used, I know, and I have a right to what are my rights. And that is something that I feel strongly.

Mr. Whittaker, in your opinion, with so many—I am sorry, Ms. Whittaker, so many variations of accuracy in the technology, what can we do that will say that we will take out these biases. We know that there have not been the algorithms. What can we do as a Congress to ensure that we are stopping this?

Ms. WHITTAKER. Thank you for the question.

I think, you know, when we talk about this technology racing forward, I think we have had an industry that has raced forward selling these technologies, marketing these technologies, making claims to accuracy that end up not being totally accurate for everyone. What we have not seen is validation race forward. We have not seen public understanding and new mechanisms for real consent, not just a sort of notice equals consent.

So, I think we need to pause the technology and let the rest of it catch up, so that we don't allow corporate interests and corporate technology to race ahead to be built into our core infrastructure without having put the safeguards in place.

Mrs. LAWRENCE. Now, the police chief in Detroit submitted a record, and I said this to him face-to-face. And he made a promise that there will never be a trial in court based solely on facial recognition. There should be something in our civil rights law and our justice system that does not allow a person to be persecuted, based on the fact that we know this data is not accurate and it has biases based on facial recognition. And that is something I think we as a Congress should do.

Thank you. My time is expired.

Chairwoman MALONEY. Thank you. You raised a lot of very good points.

The gentleman from Ohio, Mr. Jordan, is now recognized for questions.

Mr. JORDAN. Thank you, Madam Chair.

Ms. Whittaker, it is wrong sometimes, isn't it? And it is disproportionately wrong for people of color. Is that right? And this all happens—it is my understanding this all happens in a country, in the United States, where we now have close to 50 million surveillance or security cameras across the Nation. Is that right? You can say yes. You don't have to just nod. Yes, okay.

And we talked earlier about context. I think a number of witnesses have talked about context, and you know, there is the context of opening your phone is different than your apartment complex having a camera there, when we are talking about in the private sector. But it seems to me the real context concern is what is happening in—as a number of my colleagues have pointed out, what is happening with the Government and how the Government may use this technology. And we know the American Bar Association said facial recognition was used by Baltimore police to monitor protesters after the death of Freddie Gray a few years ago in the city of Baltimore, which is scary in and of itself.

And then, of course, you had five bullet points, I think, and I appreciate what you are doing with the institute that you co-founded. But point number five you said this, "Facial recognition poses an existential threat to democracy and liberty." That is my main concern is how Government may use this to harm our First Amendment and Fourth Amendment liberties.

So, and you have got to think about context even in a broader sense. I think we have to evaluate it in light of what we have seen the Federal Government do in just the last several years. You know how many times the FBI lied to the FISA court in the summer of 2016 when they sought a warrant to spy on a fellow American citizen? Are you familiar with Mr. Horowitz's report from last month, Ms. Whittaker?

Ms. WHITTAKER. I am. I don't remember the exact number.

Mr. JORDAN. Seventeen times. Seventeen times they misled a court, where they go to the court, and there is no advocate there looking out for the rights of the citizen who is going to lose their liberty, who is going to be surveilled on. And 17 times they misled the court. And we found out it was worse than we thought. They didn't spy on one American. They spied on four Americans associated with the Presidential campaign. That has probably never happened in American history.

So, when we talk about context, it is not just how facial recognition can be used by the Government. We already know it has been. It was used in Baltimore to surveil protesters. And you view it in a broader context, where the FBI went after four American citizens associated with the Presidential campaign, and we know they misled the court in the initial application and through renewals 17 times. And of course, that is after what happened a decade ago.

A decade ago, the IRS targeted people for their political beliefs. There was no facial recognition technology there. They just did it. Went out and targeted groups. Asked them questions like "Do you pray at your meetings? Who are the guests at your meetings?" before they could get a tax-exempt status.

So, this is the context. And so when we talk about why we are nervous about this, context is critical. And the context that is most critical and most concerning to, I think, Republicans and Democrats on this committee and, frankly, all kinds of people around the country who have taken some time to look into this a little bit is how the Government will use it and potentially violate their most basic liberties. And that is what we are out to get.

And you said in your testimony—you said in your testimony, you are for—bullet point number five, "It is time to halt the use of facial recognition in sensitive social and political contexts." Can you elaborate a little bit on that? What do you think that—when you say "halt," are you looking for a just flat-out moratorium on Government expanding it, stopping its use? What would you recommend, Ms. Whittaker?

Ms. WHITTAKER. Thank you for that question and that statement.

Yes, I would recommend that. I would also recommend that the communities on whom this is going to be used have a say in where it's halted and where it may be deployed. Are the people who are the subjects of its use comfortable with its use? Do they have the information they need to assess the potential harm to themselves and their communities? And is this something that—have they been given the information they need to do that?

Mr. JORDAN. Are you talking in a private sector context? Like I think the reference would be like an apartment complex and whether you can enter versus a key or some kind of fob or something, it be that, or are you talking—explain to me—elaborate on that if you could?

Ms. WHITTAKER. Yes, absolutely. You know, I am talking about both. And I think the Baltimore PD example is instructive here because the Baltimore PD was using private sector technologies. They were scanning Instagram photos through a service called Geofeedia that gave them feeds from Freddie Gray protests.

They then were matching those photos against their Faces facial recognition algorithm, which is a privately developed facial recognition algorithm, to identify people with warrants, whom they could then potentially harass. So, there is an interlocking relationship——

Mr. JORDAN. Sure.

Ms. WHITTAKER [continuing]. as I say in my written testimony, between the private sector, who are essentially the only ones with the resources to build and maintain these systems at scale, and the government use of these systems. So, there's two levels of obscurity. There is law enforcement exemption, military exemption, where we don't get the information about the use of these technologies by government, and then there is corporate secrecy. And these interlock to create total obscurity for the people who are bearing the costs of these violating technologies.

Mr. JORDAN. Thank you. My time has expired. I appreciate it, Madam Chair.

Chairwoman MALONEY. Thank you. The gentleman from California, Mr. Gomez, is now recognized for questions.

Mr. GOMEZ. First, every time I listen to a discussion on facial recognition, more and more questions emerge. It is amazing. I would like to thank my colleagues on both sides of the aisle. I know folks think that Democrats don't care about liberties or freedoms, but we do. But we also care about not only the public space, but also in the bedroom and over one's body, right? That is the way I kind of approach this issue, from a very personal perspective.

I made my concerns about this technology pretty clear. You know, the dangers it imposes on communities of color when used by law enforcement, racial bias in artificial intelligence. And as I was looking into it, Amazon continues to come up because they are one of the most aggressive marketers of this new technology. And they do it under a shroud of secrecy.

I want to be clear. I know that this technology isn't going anywhere. It is hard to put limits on technology, especially when using the law. And I have seen this time and time again, coming from California, where you have large companies understand that the wheels of government turn slowly. So, if they can just move quickly, they will outpace, outrun the government in putting any kind of limitations. You have seen this with some scooter companies who dump thousands of scooters on the street, no regulations, and then all of a sudden, it forces the government to react.

But we will react, and we will start putting some limitations on it. I know that it is tough, but there are a lot of questions. One of the things that I have been trying to figure out, what agencies—like what companies, what agencies, what Federal authorities are using it? How are they using it? Who sold it to them? And if there is a third-party validator, like NIST, who has evaluated its accuracy. Because when this technology does make a mistake, the consequences can be severe.

According to the NIST study, it said an identification of application such as visa or passport fraud detection or surveillance of false positive to match another individual could lead to a false accusation, detention, or deportation. Dr. Romine, the recently released NIST study found that facial recognition technology not only makes mistakes, but the mistakes are more likely to occur when an individual identified are racial minorities, women, children, or elderly individuals. Is that correct?

Mr. ROMINE. For most algorithms we tested, that's correct.

Mr. GOMEZ. Did your study find that these disparities were limited to just a few developers, or was the bias in accuracy more widespread?

Mr. ROMINE. It was mostly widespread, but there were some developers whose accuracy was sufficiently high that the demographic effects were minimal.

Mr. GOMEZ. Are you aware if—I know Ms. Whittaker answered this question, but has Amazon ever submitted their technology for review?

Mr. ROMINE. They have not submitted it, but we have had ongoing discussion with them about how we can come to an agreement about their submitting the algorithm. It's an ongoing conversation, so it's an active conversation that we're still having.

Mr. GOMEZ. How long has it been ongoing?

Mr. ROMINE. I don't know exactly, but it's been some months at least.

Mr. GOMEZ. OK. And you know, this is in the context of them trying to put out a blog post, and that blog post regarding their principles that you are referring to was in response to a letter that myself and Senator Markey sent to them. And you would think that it would be more than just a blog post. You would think that it would be something more serious and rises to the level of our concerns.

But with that, want to ask, Ms. Leong and Ms. Whittaker, I want to ask each of you, can you each discuss the implications of the newly released NIST report on the use of facial recognition software? What are the potential harms of using biased systems?

Ms. LEONG. I think the benefit of the report is that it discloses the bias that is present in many of the algorithms being used and gives consumers, both as individuals or businesses who might be selecting these algorithms for use, you know, good information on which to make their choices.

I want to just make the point that even though a large number of algorithms were tested, those are not equally spread across the market in terms of representing market share. The vast majority of the market right now at the high end—and particularly, that is government contracts at Federal, state, and local levels, as well as the high-end, commercial uses, like the NFL or sport stadiums or venues or amusement parks or things like that—overwhelmingly already employ the algorithms that are at the top end of this spectrum and that have very low error rates. So, it's not an evenly distributed problem, and that's part of the problem is understanding where the algorithms are being used and by whom that are causing the most harm.

Mr. GOMEZ. Ms. Whittaker? And with that, it will be my end, but I will let you answer.

Ms. WHITTAKER. Thank you.

Absolutely, I think it's important to emphasize, as Mr. Jordan did, that accurate facial recognition can also be harmful. So, bias is one set of problems, but this goes beyond that. I think any place where facial recognition is being used with social consequences, we will see harm from these racially and gender biased disparate impact.

So, I think we can look at the case of Willie Lynch in Florida, who was identified solely based on a low-confidence facial recognition match that was taken by an officer of a cell phone photo. He is now serving eight years based on that photo and had to struggle and was eventually denied to get that evidence released during his trial. So, we're seeing high stakes that really compromise life and liberty here from the use of these biased algorithms.

And you know, in response to the question of where they are being used, which algorithms are being used here, we don't have public documentation of that information. We don't have a way to audit that, and we don't have a way to audit whether they are—whether NIST's results in the laboratory represent the performance in different contexts, like amusement parks or stadiums or wherever else. So, there's a big gap in the auditing standards, although the audits we have right now have shown extremely concerning results.

Mr. GOMEZ. With that, I yield back, Madam Chair.

Chairwoman MALONEY. Thank you.

The gentlewoman from West Virginia, Mrs. Miller, is now recognized for questions.

Mrs. MILLER. Thank you, Chairwoman Maloney and Ranking Member Jordan.

As technology evolves, it is important that we are on top of it. I saw firsthand how they were using facial recognition when I was in China as a form of payment. I was also exposed to several concerning uses of facial recognition technology. As a committee, it is our responsibility to make sure that anything that is done in the United States is done thoughtfully and prioritizes the safety and individual security.

Mr. Parker, when I am at a busy airport, I am really glad that I have CLEAR to get through. Even though we have TSA, when you are in a hurry, it is really nice that you can use recognition and go forward. Can you elaborate on some examples of beneficial uses for consumers and businesses?

Mr. PARKER. Sure. And I'll stick, I guess, to the private sector uses, but also security and safety related. So, one really important one is protecting people against identify theft and fraud, something you may not think about. But here is how it works in many instances.

So, someone walks into a bank and asks to open a line of credit using a fake driver's license with the customer's real information. As part of the process, the teller tells them they have to have their photo taken. That comparison is made, and they determine it may not be the person that they say they are. And so they say, "I better talk to my management." By that time, the person that's going to commit fraud is probably long gone, right? But that's a really useful case for the technology that people don't think about.

Also, so I guess from our industry, facial recognition is also able to provide additional security for facility access control. It's typically to augment, though, other credentials, such as keys or cards, but these things can be shared, stolen, or simply lost. Biometric entry systems provide an additional convenience to registered users. For example, when there is—for expedited entry into an office building for commercial offices during rush times.

Another example, the technology is being used to reduce organized retail crime and theft, which has skyrocketed in recent years, hurting American businesses, consumers, taxpayers alike.

Mrs. MILLER. Do you think that the mainstream media outlets have given an honest portrayal of how this technology is utilized and the reality of its capabilities?

Mr. PARKER. And so, I don't think so. I think this is a complex issue, as we've been talking about here, and I think it tends to get oversimplified and mischaracterized. Going back to what I said earlier, I think the issue is that what's causing some concern is about how the technology is used. It's not the technology itself. And I think there's other technologies that could be used in similar ways, and so we need to think more constructively about what the rules should be about the use of many different types of technology.

Mrs. MILLER. Thank you.

Dr. Romine, I have a very good friend in West Virginia by the name of Chuck Romine, and his son is Dr. David Romine. But if we scanned both of you, you would not look anything alike. During a House Homeland Security Committee hearing on July 11, in your testimony you discussed accuracy rates across multiple demographics and how inaccurate results are diminishing. Now that you have published the report, is that still accurate, and in what other areas is this technology improving?

Mr. ROMINE. So, I hope my statement in July was that the most accurate algorithms are exhibiting diminishing demographic effects. And we certainly do believe that this, the report that we released just last month, confirms that.

Mrs. MILLER. You also stated that anytime the overall performance of the system improves, the effects on different demographics decrease as well. Is that still something that is still true to this day?

Mr. ROMINE. That is correct.

Mrs. MILLER. Good. Knowing that accuracy rates have improved within 2014 to 2018, can you further explain the role of performance rates and why they are important for the end-users of these technologies?

Mr. ROMINE. Absolutely. It's essential that in the selection of a system, you understand the algorithm that the system uses and select for an accuracy that is sufficiently robust to provide you the minimized risk for the application. In some cases, the application may have very limited risk, and the algorithm may not be important. In other cases—or as important. But in other cases, the risk may be severe, such as identification of suspects, for example, or access to critical infrastructure. If there is facial recognition being used for that, then you want to have an algorithm basis for your system that is high-performing.

Mrs. MILLER. Could you speak to where your researching techniques that exist to mitigate performance differences among the demographics and what is emerging research and standards in NIST interested in supporting?

Mr. ROMINE. Sure. Thank you for the question.

Although we didn't specify too many of the mitigations that we would expect people to adopt today, one of the things that we do want to do is to point policymakers and consumers to ways in which these things can be mitigated. One of the mitigations can be a determination of an appropriate threshold to set to ensure that any algorithm that you use, you set an appropriate threshold for the use case. Another is a possible use of a separate biometric. So in addition to face, having a fingerprint or an iris scan or some other type of biometric involved that would help to reduce the error substantially more.

Mrs. MILLER. Thank you. I yield back my time.

Chairwoman MALONEY. Thank you.

The gentlewoman from Massachusetts, Ms. Pressley, is recognized for questions.

Ms. PRESSLEY. Thank you, Madam Chair.

The use of facial recognition technology continues to grow at a breathtaking pace and is now seeped into nearly every aspect of our daily lives. Many families are unaware that their faces are being mined as they walk through the mall, the aisles of the grocery store, as they enter their homes or apartment complexes, and even as they drop their children off at school. In response, several municipalities, including within the Massachusetts Seventh congressional District, which I represent—So,merville and Cambridge, respectively—have stepped up to the plate to protect their residents from this technology.

We know that the logical end of surveillance is often over-policing and the criminalization of vulnerable and marginalized communities. It is also why I worked with my colleagues Representative Clarke and Representative Tlaib on legislation to protect those living in HUD public housing from this technology.

More recently, school districts have begun to deploy facial analytics in school buildings and at summer camps, collecting data on teachers, parents, and students alike. Ms. Leong, how widespread is the use of this technology on children in schools?

Ms. LEONG. We're seeing facial recognition systems being implemented more and more in schools. I think the actual number is still very small in terms of percentage penetration of the number of schools in this country, but it's certainly spreading and growing.

And it's one of the use cases we think is entirely inappropriate, that there's just really no good justification for a facial recognition system in a K-to–12 school. They are mostly being used in security applications, sometimes in a sort of fear-driven response to school shooter scenarios and things like that, which, in my opinion, they do not adequately address in any meaningful way and is not the best use of funds or the best way to heighten security around schools in response to those threats.

The other part of your question that was the facial characterization programs, which I think are being used more and more in an educational context, where we are seeing systems that try to evaluate are students paying attention? What's the engagement rate? What's the response rate of students to certain teachers or types of teaching or things like that?

As I think was mentioned once earlier in the hearing by someone else, that is based on very questionable data at this point, and I think in the not ready for primetime category definitely qualifies in the sense that we're seeing it very quickly applied in many use cases that the science and the research is not there to back up. And it's particularly concerning when you're talking about children in schools, not only because they're essentially a captive population, but because the labels or decisions that might be made about those children based on that data might be very, very difficult to later challenge or in any way reduce the effects on that particular child.

Ms. PRESSLEY. Well, yes, serious security and privacy concerns. Dr. Romine, your study found that the error rate of facial analytic software actually increased when identifying children. Is that correct?

Mr. ROMINE. For most algorithms, that's correct.

Ms. PRESSLEY. OK. And why was that?

Mr. ROMINE. We don't know the cause and effect exactly. There is speculation that children's faces are—have—with less life experience, there are less feature-rich faces, but we don't know that for sure because the convolutional neural networks that are used are—it's difficult to make a determination of the reason.

Ms. PRESSLEY. Got it. And many of you have mentioned in which these image data bases can be vulnerable to hacking or manipulation. Ms. Whittaker, when children's images are stored in data bases, are there any unique security concerns that they raise or that may arise?

Ms. WHITTAKER. Absolutely. Security for minors is always a concern.

Ms. PRESSLEY. OK. Well, this technology is clearly biased, inaccurate, and even more dangerous when used in schools, where black and brown students are disproportionately already over-policed and disciplined at higher rates than their white peers for the same minor infractions. In my district, the Massachusetts Seventh alone, black girls are six times more likely to be suspended from school and three times more likely to be referred to law enforcement, again, for the same infractions as their white peers. Our students don't need facial recognition technology that can misidentify them and lead them to the school-to-confinement pathway.

Last fall, I introduced the Ending PUSHOUT Act, which would urge schools to abandon over-policing and surveillance and to instead invest resources in trauma-informed supports, access to counselors and mental health professionals, resources that will really keep our kids safe. In my home state of Massachusetts, a broad coalition of educators, civil rights, and children's rights advocates are leading the fight and saying no to the deployment of facial recognition technology in our schools, and I am grateful for their activism and their solidarity on this issue.

I would like to include, pardon me, for the record a letter from the BTU, the NAACP, AFT Massachusetts, MTA, the AFCLU Massachusetts, and many others, urging our state to reject additional surveillance and policing in our schools.

Chairwoman MALONEY. Without objection, so ordered.

Ms. PRESSLEY. Thank you. And I yield.

Chairwoman MALONEY. Thank you.

And the gentleman from North Dakota, Mr. Armstrong, is now recognized for questions.

Mr. ARMSTRONG. Thank you, Madam Chair.

I think there are a couple things that we should talk about for a second because I think they are important. And one of them—I am going to go to the Fourth Amendment and criminal context and how this could be deployed there. And this isn't the first time we have seen the crisis in Fourth Amendment. It happened with telephoto lenses. It happened with distance microphones, GPS trackers, drones, and now we are at facial recognition. And to be fair, the Fourth Amendment has survived over time pretty well, but biometric information has a different connotation, which I will get to in a second.

I also agree with Ranking Member Jordan that we can't leave this for the courts to decide. And one of the reasons we can't is the courts are going to take a constitutional view of privacy, not a popular culture view of privacy. And so when we are into the civil context and data sharing and these types of issues, I will be the first to admit, my facial recognition didn't work on my phone over Christmas. You know what I did? Drove immediately to the cell phone store and got a new one. So, I understand the convenience of it and those things.

But the Carpenter case is a pretty good example of how at least the U.S. Supreme Court is willing to change how they view privacy in the digital age. So, part of our job as Congress is to ensure that we write a law and write regulations that ensure that we can maintain those types of privacy standards.

Now one of the reasons biometric—and I wish some people were here—is a little different is because there is one unique thing in a criminal case that is really, really relevant to facial recognition, and that is identity cannot be suppressed. I can suppress a search. I can suppress 40 pounds of marijuana. I can suppress a gun. I can suppress a dead body. But you cannot suppress identity.

So, as we are continuing to carve through these, one thing I think we have to absolutely understand is in these types of cases, we need to apply a statutory exclusionary rule. Otherwise, any regulations we pass don't really, truly matter in a courtroom. And two, we have to figure out a way for meaningful human review in these cases.

Because when they say, we will never prosecute somebody solely on facial identity, well, that is a fair statement, except there has to be an underlying offense of a crime, so they are prosecuting them on something else as well. And it is really, really important.

But I also think it is important to recognize that not all populations are the same. There is a big difference between using facial recognition in a prison setting and even, quite frankly, in a TSA or a border setting than there is for a law enforcement officer walking around the street with a body camera or people getting profiled at a campaign rally. And so we have to continue to have those conversations.

But I also want to point out that one of the things we have to do when we are dealing with these types of things in the law enforcement scenario, and I don't care what law enforcement it is—state, local, Federal, DEA—all of those issues have to figure out a way to account for false positives.

And the reason I say that is, and I am going to use a not an apples-to-apples analogy, but in North Dakota, highway patrolmen have drug dogs. Not all of them, but some of them, and they are multi-use. I mean, our law enforcement usually has those.

So, if you are speeding down the street or speeding down the highway going 75 in a 55, and you get pulled over and that highway patrolman happens to have a drug dog in his car, and he walks that drug dog around your car and that dog alerts, and they search your car and they don't find any drugs and they let you leave, and they give you your speeding ticket and you go along your way, that data never shows up in that dog's training records. It never shows up.

So, when you are talking about the accuracy of a drug dog, when you are talking about the accuracy of finding a missing girl, or any of those issues, we cannot wait until that situation arises. Because if there is a missing girl on the Mall out here, I will be the first one standing at the top of the Capitol steps saying use whatever technology to deploy. Grab everybody you can. Let's find this little girl. And I agree with that there. But you cannot have meaningful regulation unless you have meaningful enforcement.

And one of the concerns I have when deploying this technology in a law enforcement setting is it is very difficult, by the nature of how that works, to deal with those false positives. Like my questions are when we are talking about the missing girl or the rice cookers is, how many people were stopped? How many people were stopped that weren't that person? I am glad they found her. I am glad they caught the guys.

But we have to be able to have a situation in place where we can hold people accountable. And the only ways I can think of to do that is to continue to develop this. One, use it in populations, where—I mean, and perfect it.

Now the problem with the prison population is you have a static population. The problem with the Mall outside is it is a completely variable population. But I think when we move forward with this, and particularly in a law enforcement and criminal setting, we have to recognize the fact that you cannot suppress identity.

So, it is different than a lot of other technologies. Because if your number is 90 percent and you stop somebody at 60 percent and it still happens to be that person, under current criminal framework, they are not—I can make that motion, the judge will rule in my favor, and say, "Too bad, still arrested." So, with that, I yield back.

Chairwoman MALONEY. Thank you.

The gentlewoman from Michigan, Ms. Tlaib, is now recognized for questions.

Ms. TLAIB. Thank you, Madam Chair.

I think many of you probably already know I am particularly disturbed by the aspect of facial recognition technology being used by landlords and property owners to monitor their tenants, especially in public housing units. In Detroit, for example, the city's Public Housing Authority recently installed security cameras on these public housing units that we believe is going to be something that encroaches onto people's privacy and their civil liberties.

You know, these are people's homes. And so, I don't think being poor or being working class means somehow that you deserve less civil liberties or less privacy. And so, Ms. Leong, what are the privacy concerns associated in enabling facial recognition software to monitor public housing units? If you live in a low-income community, is your civil liberties or your privacy lessened?

Ms. LEONG. Thank you for the question. And of course not. At least hopefully not.

I think this is a great example of the conversation that needs to happen at the beginning of this, which is what is the problem that they're trying to solve by putting this into a housing complex, any housing complex? What is the landlord or the owner's gain? What is it they're trying to do? Is it convenience? Is it some level of security? Is it just because it's a really cool technology that they offered him on a discount, and he wants to use it? What is he trying to gain from it?

And then with that in mind, what are the risks to the occupants? In my opinion, that would be a commercial use, which would mean that even if it was installed, it would be only for those residents who chose to opt in and enroll and use it as their way in and out of the building. But for residents who didn't want to, they would not be enrolled in the data base and should not be included in that.

But certainly, from a civil liberties point of view, if this was being used in some way, the other laws about inequitable impact or protected classes don't go out the window just because you use a new technology. They are still in place, still need to be applied. It's sometimes a new way of evaluating them because of new technologies, and so they raise challenging questions——

Ms. TLAIB. Ms. Leong, these new technologies, they are for profit, right?

Ms. LEONG. The company who designs them——

Ms. TLAIB. Yes.

Ms. LEONG [continuing]. sells them for profit.

Ms. TLAIB. They are for-profit technology that are coming into communities like mine that is overwhelmingly majority black and testing these products, this technology, onto people's homes, the parks, the clinics. It is not stopping. Now I hear my good colleague from Massachusetts talk about them installing it in schools.

They are using this, and I have a police chief that says, oh, this is magically going to disappear crime, but if you look, my residents don't feel less safe. They actually don't like this green light that is flashing outside of their homes, the apartment building, because for some reason he is telling everybody it is unsafe here. You know, it takes away people's kind of human dignity when you are being policed and surveillanced in that way.

Now, and this is a question for Dr. Romine, they are now trying to say we are going to use facial technology as like the what do they call, the key fobs. They want to now use access to people's homes using facial recognition technology on key fobs. So, you know, one of the consequences of that is misidentification. I mean, my colleague on the other side just talked about how he couldn't even access his phone. I am really worried that they are testing my people, my residents are being used as testing ground for this kind of technology, of using it as a key fob. Do you have any comment in regard to that?

Mr. ROMINE. The only comment I have from the NIST perspective is that the algorithm testing that we do is to provide information to people who will make determinations of what is and is not an appropriate use. That includes this—you know, this committee, any potential regulation or lack of regulation, and any deployment that's made in the private sector or otherwise is outside the purview of NIST.

Ms. TLAIB. Well, I am really proud to be co-leading with Congresswoman Pressley, as well as Congresswoman Yvette Clarke, and leading No Biometric Barriers to Housing Act, which would prohibit any—you know, completely ban facial recognition technology on Federal-funded housing buildings and properties. We should be very careful. I think Congressman Mark Meadows is right.

You know, I hear some of my colleagues on both sides say, well, we got to fix the algorithms, we got to do this. I said, well, I am not in the business and we shouldn't be in the business of fixing for-profit technology industries, you know, these new, you know, they call them tools. They give them all these great names, but they are processes in place of, you know, human contact, police officers on the street.

I increasingly talk about this with, you know, the police chief and others, and all they can say is, well, we did this, and we were able to do that. But like my colleague said, how many people did you have to go through? Because I watched while they matched a suspect with 170-plus people. I watched as they took a male, a male suspect and matched him with a female. One hundred and seventy, I watched.

And the kind of misleading the public of saying, well, you must not care about victims. No, I actually do care about victims. How about the victim that you are just now misidentifying, you are increasing?

And so, with that, Chairwoman, I do really want—and I hope you all read this—but a report by the Detroit Community Technology Projects. It is a Critical Summary of Detroit's Project Greenlight and its greater contacts and the concerns with the use of facial recognition technology in Detroit. I would like to submit it for the record.

Chairwoman MALONEY. Without objection.

Ms. TLAIB. Thank you, and I really do appreciate all of your leadership on this. And thank you so much, Chairwoman, in doing yet a third hearing on this and continuing this critical issue that I know was important to Chairman Cummings. Thank you very much.

Chairwoman MALONEY. The gentleman from Kentucky, Mr. Comer, is now recognized for questions.

Mr. COMER. Thank you. And I ask that you bear with me. I am battling laryngitis. So, laryngitis with a bad accent doesn't spell success.

[Laughter.]

Mr. COMER. I think there is bipartisan concern here today for facial recognition technology as we move forward. My first question is for Dr. Romine, with respect to the National Institute for standards testing. What is NIST's role in establishing Government-wide policy?

Mr. ROMINE. The only role that we have with respect to Government-wide policy is providing the scientific underpinning to make sound decisions. And so as a neutral, unbiased, and expert body, we are able to conduct the testing and provide the scientific data that can be used by policymakers to make sound policy.

Mr. COMER. Well, how does a NIST technical standard differ from a policy standard?

Mr. ROMINE. Well, certainly technical standards can be used by policymakers. So, in this case, a determination of a policy that was predicated on identification of algorithms that are based on their performance characteristics is—would be one example of that. But from a policy perspective of what to do or what not to do with face recognition technology, that's something we would support with scientific data, but not with policy proclamations.

Mr. COMER. Let me ask you this. Is NIST the right agency to develop Government-wide policy?

Mr. ROMINE. I don't think so, sir. I don't think that's a NIST role.

Mr. COMER. OK. What is NIST's role in developing accuracy standards for facial recognition technology?

Mr. ROMINE. Our role is in evaluating the accuracy, and in particular, one of the things that we've developed over the last 20 years is the appropriate measurements to make. These measurements didn't exist. We worked with the community to develop a set of technical standards for not just the measurement itself, but how to measure these things, including the reporting of false positives, false negatives, the very detailed definition of what those constitute.

Mr. COMER. Thank you.

Mr. Parker, I understand that the Security Industry Alliance supports the U.S. Chamber of Commerce's recently released facial recognition policy principles. What are the principles, and why do you support them?

Mr. PARKER. Yes. Thank you for the question.

Yes, so I think that the Chamber put a lot of really great work into developing this framework. And basically, it mirrors some of the work that was done earlier by the Department of Commerce NTIA.

They had convened a multi-stakeholder process that included industry, but also other parties from the commercial sector about what does appropriate commercial use look like. And I think, you know, some of the principles have to do with, you know, transparency is obviously the main one, but also, as we were discussing earlier, what should be done as far as opt-in consent in the commercial setting. I think that's going to cover most cases, for example.

Mr. COMER. Well, can you describe how those principles balance the need for protecting civil liberties while also promoting industry innovation?

Mr. PARKER. Well, I think for the commercial use, we're primarily talking about data privacy. So, that's a little different. Civil liberties concerns surround Government use primarily.

Mr. COMER. Well, let me followup, and this will be my last question. What does the path ahead look like for these principles?

Mr. PARKER. So, I think that the debate going on right now about establishing a national framework for data privacy is a really important one. And I think that how to set rules for use of the technology in the commercial setting, it's within that framework. And so, I know we've had the GDPR in Europe, but also in the United States, we have some states that are establishing their own frameworks. And that could be a real problem for our economy if we don't establish standardized rules.

Mr. COMER. OK. Thank you.

Madam Chair, I yield back the balance of my time.

Chairwoman MALONEY. Thank you.

The gentleman from Virginia, Mr. Connolly, is now recognized for questions.

Mr. CONNOLLY. I thank the chair.

And thank you all so much. It has been a stimulating conversation. It just seems to me, you know, we are going to have to really grapple with what are the parameters of protecting privacy and controlling the use of this technology. And one of the traps I hope, on my side of the aisle particularly, we don't fall into is continuously citing the false IDs. Because if we make the argument this technology is no good because there are a lot of false IDs, that may be true today and the concern is legitimate, but technology's nature is it will improve.

So, what will we say when it becomes 95 percent accurate? Then what? Are we conceding the argument that, well, then you can used it with impunity?

I would certainly argue, irrespective of its accuracy, there are intrinsic concerns with this technology and its use. And maybe we have to look at things like opt-in and opt-out, where you actually require the consent of anybody whose face is at issue to be able to transfer it to another party whether you are Government or not Government.

Mr. Parker, you were talking about primarily being concerned about how Government uses facial recognition technology, but do we have any reason to believe the private sector might also generate some concerns?

Mr. PARKER. Sure. That's why we need to establish best practices about how it's used, you know, particularly in any applications where there is any kind of serious consequence for errors, you know, for example.

Mr. CONNOLLY. Errors. Well, let me give you a different example. So, IBM got a million photos from a photo hosting site called Flickr. It sent the link to that data base, a million faces, to Chinese universities.

Now that wasn't the Government doing it. It was a private entity. And it wasn't about accuracy, it was about an entire dataset going to a foreign adversary who has a track record of actually using this technology to suppress and persecute minorities, for example, Uyghurs, to wit. We know they are doing that.

So, might you have any concern about a company like IBM engaging in that kind of behavior, in transferring an entire dataset to Chinese universities with close ties, obviously, to the Chinese government?

Mr. PARKER. Yes, certainly. And I think we've seen this reflected in U.S. Government policy, too, which established a restriction on exports to a number of Chinese companies, particularly those that are developing this technology that we're talking about.

Mr. CONNOLLY. Ms. Whittaker, your views about that?

Ms. WHITTAKER. Well, I think that highlights one of the issues that trying to implement consent raises, which is that those photos are already on Flickr. Those are photos that someone may have put on Flickr during a very different Internet, when facial recognition at scale was not a technical possibility the way it is today. And they are now being scraped by IBM. They are being scraped by many, many other researchers to comprise these datasets that are then being used to train these systems that may be erroneous, that may target our communities, and that may violate our civil liberties.

So, where we ask for consent, how consent could work, given that we have a 20-year history where we've clicked through consent notifications without reading them as a matter of habit to get to the core technical infrastructures of our lives, remains a big, open question. And I think we would need to be able to answer that.

Mr. CONNOLLY. Certainly, I think we could agree, could we not, that whether I clicked consent for Flickr or any other entity to have access to and within reason use my photo, I never contemplated having that photo transferred to a foreign government or to a university with close ties to a foreign government?

Ms. WHITTAKER. Yes, or to have a corporation use it to train a system that they might sell to law enforcement in ways that targets your community.

Mr. CONNOLLY. Right.

Ms. WHITTAKER. There's a lot of things we did not consent to.

Mr. CONNOLLY. Well, it just seems to me, Madam Chairman, that this being the third hearing where we all have expressed concern about the zone of privacy and, frankly, informed consent about citizens or noncitizens whose data—in this case, their face—may be used and how it may be used and transferred to a third party, we have got some work to do in figuring out the rules of engagement here and how we protect fundamental privacy rights of citizens. Unless we want to go down the road of expanding and transferring—excuse me, transforming the whole definition of the zone of privacy. And that is a very different debate. But it seems to me that we can't only concede the technology will drive the terms of reference for privacy.

Thank you, Madam Chairman.

Chairwoman MALONEY. Thank you.

The gentleman from Wisconsin, Mr. Grothman, is now recognized for questions.

Mr. GROTHMAN. OK. Maybe I will start with Ms. Whittaker, but anybody else can jump in if they want, I guess. Could you go over a little bit the degree or how this technology is being used in China today?

First of all, though, I would like to thank Mr. Connolly for his comments. I think the inference that the major problem here is getting false information is, I don't think, the biggest concern. I think the biggest concern is it becomes more and more—it is better and better as the evil uses that it is used for. And some of my colleagues seem to imply that as long as we are not getting any false information, apparently, the more information we have, the better. I think sometimes the less information the Government has, the better.

But, OK, Ms. Whittaker, go ahead.

Ms. WHITTAKER. Absolutely. Thank you for the question.

I want to preface my answer by saying that I am an expert on artificial intelligence, and I understand the tech industry very well. I'm not a China expert. However, it is very clear that these technologies are being used in China to implement social control and the targeting of ethnic minorities. You have networks of facial recognition systems that are designed to recognize individuals as they go about their daily lives and issue things like tickets if they jaywalk, if they are recognized by a facial recognition system.

Mr. GROTHMAN. Could it be used—people attend religious ceremoneys in China, would it be used there?

Ms. WHITTAKER. Absolutely. The same way that Baltimore police used it to look at people who attended a Freddie Gray protest. It's the same principle. You're just seeing it deployed in a different context.

Mr. GROTHMAN. I attended a rally last night for President Trump. I think about 12,000 people were there. Do you think it is possible that any facial recognition technology was being used there, so people would know who was showing up at the rally, who was hanging around outside before the rally?

Ms. WHITTAKER. The capacities in technological affordances certainly exist. Again, the type of obscurity within which these technologies are deployed by both the Government and the private sector makes it very difficult to speculate beyond that because we are just not told when it's used and where.

Mr. GROTHMAN. Would it surprise you if it was being used there?

Ms. WHITTAKER. No.

Mr. GROTHMAN. OK. There is the concern I have. And we have a Government that has weighed in against certain people. The ranking member pointed out the IRS in the past has shown strong bias against conservatives, okay, and we use the power of Government against conservatives. We had a major Presidential candidate a while ago saying he wants to take people's guns. And so you got to worry, you know?

Would it surprise you if facial recognition technology was being used—I am going to attend a gun show this weekend in my district. Would it surprise you if facial recognition technology was being used to develop a data base of people going in that gun show?

Ms. WHITTAKER. Facial recognition is being used to develop or against many different kinds of data bases.

Mr. GROTHMAN. OK. Kind of concerning there. To me, that is the major concern, that our country will work its way toward China, as we have—I think a while back we had a Presidential candidate, you know, hostilely question a prospective judge because they were a member of the Knights of Columbus, which is kind of scary. Could you see the day coming in which we are using facial technology to identify which people are, say, attending a Catholic Church? That apparently seems to bother some people.

Ms. WHITTAKER. Again, that's the same principle as the Baltimore Police Department using it to see who attends a Freddie Gray rally and target them if they have a warrant. So, it is already being used in that capacity, irrespective of which group it's targeting or not.

Mr. GROTHMAN. If you set up a Catholic Church in China, do you think the Red Chinese government would probably be trying to use facial recognition technology to know in the future who is a member of that church? I don't know if they have any Knights of Columbus chapters in China, but you know, identifying in China if you would show up at a Knights of Columbus meeting?

Ms. WHITTAKER. Again, the technological capabilities exist, but I am an artificial intelligence expert, not a Chinese geopolitical expert.

Mr. GROTHMAN. Anybody else want to comment on what is going on in China?

Ms. WHITTAKER. I think it is a model for authoritarian social control that is backstopped by extraordinarily powerful technology. I think one of the differences between China and the U.S. is that their technology is announced as state policy. In the U.S., this is primarily corporate technology that is being secretly threaded through our core infrastructures without that kind of acknowledgment.

Mr. GROTHMAN. Right. Amazon a big player here?

Ms. WHITTAKER. Absolutely. Amazon is one of the big——

Mr. GROTHMAN. They are a very political group, aren't they? Or they have expressed strong political opinions?

Ms. WHITTAKER. They certainly hire many lobbyists.

Mr. GROTHMAN. OK. I think they have—okay. Thank you for giving me an extra few seconds.

Chairwoman MALONEY. Thank you.

The gentlelady from New York, Ms. Ocasio-Cortez?

Ms. OCASIO-CORTEZ. Thank you, Chairwoman Maloney. And thank you again for holding a third hearing on something that is so important and is such an emerging technological issue that it is really important for the public to understand.

We have heard a lot about the risk of harm to everyday people posed by facial recognition, but I think it is important for people to really understand how widespread this is. Ms. Whittaker, you made a very important point just now that this is a potential tool of authoritarian regimes, correct?

Ms. WHITTAKER. Absolutely.

Ms. OCASIO-CORTEZ. And that authoritarianism or that immense concentration of power could be done by the state, as we see in China, but it also could be executed by mass corporations, as we see in the United States, correct?

Ms. WHITTAKER. Yes.

Ms. OCASIO-CORTEZ. So, can you remind us, Ms. Whittaker or Ms. Leong, can you remind us of some of the most common ways that companies collect our facial recognition data?

Ms. WHITTAKER. Absolutely. They scrape it from sites like Flickr. Some use Wikipedia. They collect it through massive networked market reach. So, Facebook is a great example of that.

Ms. OCASIO-CORTEZ. So, if you have ever posted a photo of yourself to Facebook, that could be used in a facial recognition data base?

Ms. WHITTAKER. Absolutely. By Facebook and potentially others.

Ms. OCASIO-CORTEZ. If you have posted it to Wikipedia?

Ms. WHITTAKER. Yes.

Ms. OCASIO-CORTEZ. Could using a Snapchat or Instagram filter help hone an algorithm for facial recognition?

Ms. WHITTAKER. Absolutely.

Ms. OCASIO-CORTEZ. Can surveillance camera footage that you don't even know is being taken of you be used for facial recognition?

Ms. WHITTAKER. Yes, and cameras are being designed for that purpose now.

Ms. OCASIO-CORTEZ. And so, currently, cameras are being designed. People think, you know, I am going to put on a cute filter and have puppy dog ears and not realize that that data is being collected by a corporation or the state, depending on what country you are in, in order to track you or to surveil you, potentially for the rest of your life. Is that correct?

Ms. WHITTAKER. Yes.

Ms. OCASIO-CORTEZ. Do you think average consumers are aware of how companies are collecting or storing their facial recognition data?

Ms. WHITTAKER. I do not.

Ms. OCASIO-CORTEZ. And what can a consumer or a constituent like mine do if they have been harmed by companies' improper collection? In a previous hearing, we were talking about how facial recognition oftentimes has had the highest error rates for black and brown Americans, and the worst implications of this is that a computer algorithm will tell a black person that they have likely committed a crime when they are innocent. How can a consumer or a constituent really have any sort of recourse against a company or an agency if they have been misidentified?

Ms. WHITTAKER. Right now, there are very few ways. There is the Illinois Biometric Information Privacy Law that allows private actors to bring litigation against companies for corporate misuse of biometric data. But, one, you have to know it's been collected. Two, you have to know it's been misused. And three, you have to have the resources to bring a suit, which is a barrier to entry that many of those most likely to be harmed by this technology cannot surpass.

Ms. OCASIO-CORTEZ. So, let's say if you walk into a technology store, or as this technology spreads, you just walk into a store in the mall, and because the error rates for facial recognition are higher for black and brown folks, you get misidentified as a criminal. You walk out, and let's say an officer stops you and say someone has accused of a crime, or we think that you have been accused of a crime. You have no idea that facial recognition may have been responsible for you being mistakenly accused of a crime. Is that correct?

Ms. WHITTAKER. That's correct. And we have evidence that it's often not disclosed.

Ms. OCASIO-CORTEZ. And so that evidence is often not disclosed, which also compounds on our broken criminal justice system, where people very often don't get entitled to the evidence against them when they are accused of a crime. Is that correct?

Ms. WHITTAKER. Yes, the Willie Lynch case in Florida is case in point.

Ms. OCASIO-CORTEZ. So, what we are seeing is that these technologies are almost automating injustices, both in our criminal justice system, but also automating biases that compound on the lack of diversity in Silicon Valley as well?

Ms. WHITTAKER. Absolutely. These companies do not reflect the general population, and the choices they make and the business decisions they make are in the interest of a small few.

Ms. OCASIO-CORTEZ. So, you know, Madam Chairwoman, I would say this is some real-life Black Mirror stuff that we are seeing here. And I think it is really important that everyone really understand what is happening because this is—and as you pointed out, Ms. Whittaker, this is happening secretly as well, correct?

Ms. WHITTAKER. Yes.

Ms. OCASIO-CORTEZ. All right. Thank you. And that is my time.

Chairwoman MALONEY. Thank you.

The gentleman from Pennsylvania, Mr. Keller, is now recognized for five minutes.

Mr. KELLER. Thank you, Madam Chair.

And I just want to say that we all represent many people that are probably not familiar with the commercial and the Government's use of the facial recognition technology. I mean, there is a lot of technology out there. So, I am grateful for the witnesses being here to help shed a little bit of light on the topic of facial recognition technology.

And when we look at the—if there is a proper approach toward regulating the use of facial recognition technology, you know, we need to balance personal privacy with whatever appropriate use there may be as a tool to make, you know, the Government or law enforcement capabilities more effective in what they do. And the reason I say this is several years ago something happened in the legal community called the "CSI effect," where television shows exaggerated the prevalence of DNA and forensic evidence and the ease of its processing in criminal cases. You know, defense attorneys then used the public's new perception of this evidence to claim the lack of enough forensic evidence meant that the police didn't do their due diligence.

You know, today many law enforcement television shows and movies utilize, you know, and they reference facial recognition technology as part of their storytelling. You know, so there are a lot of concerns here. And you know, I have concerns with, you know, the Fourth Amendment and all of our rights that we have.

And I guess, Mr. Parker, if you could just maybe explain to what extent do you think the current pop culture is filled with an exaggerated or distorted view of how prevalent the use or if there is an appropriate use of facial recognition technology?

Mr. PARKER. Yes, I guess, first of all, I do think that it has—I mean, if you look at the portrayal of the technology in the media, it's far beyond what we can do right now. So, that's one thing to consider. I think the other thing is that, you know, we mentioned earlier about, you know, what's happening in China. Unfortunately, their government by policy is using technology, not just this one, many others to persecute certain groups. And obviously, that's a horrible example of how technology can be misused.

So, I think also the capability is different there. I'm not an expert on China either, but you know, to use a facial recognition system, there has to be a data base with people enrolled in it, you know? And so, you know, I suspect there is a large data base like that over there.

But I can speak on behalf of our members. You know, we have no interest in helping the Government at any level here do mass surveillance of citizens engaged in lawful activity. We have no interest in that. And that's not the case right now as a system, and I haven't seen evidence that that's what's intended, but certainly that's not a place we want to go.

Mr. KELLER. Yes. And you mentioned, you know, technology can be a great tool, and it can. And it goes with anything. Our phones can keep us very well-connected and do things. It can become a great hindrance and distraction, too, and be used for a lot of malicious and evil things. I mean, a lot of people now bully using, you know, social media and so on. So, that can happen with anything, and it is a matter of how we effectively regulate that and make sure it doesn't get used inappropriately.

Also, Mr. Parker, do you think we could be looking at the possible new CSI effect in terms of facial recognition and the use of law enforcement? Do you think that——

Mr. PARKER. Yes, so that is a risk. And I think you are right to identify that. I think the key here is to have really locked down and thorough use policies and constraints. I think there's many uses in both the private sector and the public sector where that is being done correctly. There are other cases we know less about because there is less transparency. But making—you know, part of that is some accountability measures that ensure use of those systems are auditable to make sure that they are only being used for the purposes specified by the people who have authorization to do it.

Mr. KELLER. OK. I appreciate that because this is a very sensitive issue, and I do appreciate the opportunity of having these hearings so that more people are aware of what is happening.

Thank you, and I yield back.

Chairwoman MALONEY. Thank you.

I recognize the gentlewoman from New Mexico, Ms. Haaland, for questions.

Ms. HAALAND. Thank you, Mr. Chair.

Thank you all so much for being here today. We appreciate your time and effort in this hearing.

I recently read that some employers have begun using facial recognition technology to help decide who to hire. At certain companies, such as Hilton and Unilever, job applicants can complete video interviews using their computer or cell phone cameras, which collect data on characteristics, like an applicant's facial movements, vocal tone, and word choice.

One company offering this technology, HireVue, collects up to 500,000 data points in a 30-minute interview. The algorithm then ranks the applicant against other applicants based on the so-called "employability score." Job applicants who look and sound like the current high performers at the company receive the highest scores.

Ms. Whittaker, I have two questions for you. One, isn't it true that the use of facial recognition and characterization technology in job application processes may contribute to biases in hiring practices? And, if yes, can you please elaborate?

Ms. WHITTAKER. It is absolutely true. And the scenario that you described so well is a scenario in which you create a biased feedback loop in which the people who are already rewarded and promoted and hired to a firm become the models for what a good employee looks like. So, if you look at the executive suite at Goldman Sachs, which also uses HireVue for this type of hiring, you see a lot of men, a lot of white men.

And if that becomes the model for what a successful worker looks like and then that is used to judge whether my face looks successful enough to get a job interview at Goldman Sachs, we are going to see a kind of confirmation bias in which people are excluded from opportunity because they happen not to look like the people who had already been hired.

Ms. HAALAND. Thank you so much for that.

So, Ms. Whittaker, would you agree that granting higher employability scores to candidates who look and sound like high-ranking employees may lead to less diversity in hiring then?

Ms. WHITTAKER. I would agree, and I would also say that that methodology is not backed by scientific consensus.

Ms. HAALAND. Thank you.

Ms. Leong, do you envision any privacy concerns that may arise when employers collect, store, and use the data generated from video job interviews?

Ms. LEONG. Yes. Thank you for the question.

That is absolutely a concern since the individuals may not be aware of what data is being collected, especially if some of those systems are being used maybe even in an in-person interview, but there is a camera running that's collecting some sort of characterization profile and that the person may or may not be aware of that or whether that's part of the decisionmaking process for their application.

Ms. HAALAND. Thank you so much.

So I, like many of my colleagues, have expressed, am concerned over the use of this technology. I am concerned that face recognition technology disenfranchises individuals who don't have access to Internet-or video-enabled devices, which is an awful lot of people in this country because broadband Internet is an issue in so many rural communities and other communities throughout this country.

I am worried that relying on algorithms to predict high-ranking employees will only inhibit the hiring of a more diverse work force.

Dr. Romine, your testimony today highlighted many of these risks. NIST showed that commercial face recognition algorithms misidentified racial minorities and women at substantially higher rates than white males. As Members of Congress, we must develop legislation to ensure we get the best of the benefits of this technology while minimizing the risks of bias in employment decisions.

And Chairwoman, I yield back.

Chairwoman MALONEY. That concludes our hearing. We have no other witnesses. The ranking member, I am recognizing him and others on this side of the aisle for five minutes, and then we will close with five minutes.

Mr. JORDAN. I thank the chair, and I won't take all five. Just the broad outlines of what we are trying to do legislatively sort of as a start, and we are working with the chair and with members of the majority as well, really is first just an assessment. I am talking again largely what Government is doing, what the Federal Government is doing.

So, the first thing we would like to ask for is we just want to know which agencies are using this? How they are using it? To what extent is it happening? And as I think several of you testified, but certainly Ms. Whittaker, we just don't know that. We don't know to what extent is the FBI using it. To what extent are other agencies using it, IRS, any other agency?

We found out a few years ago the IRS was using stingray technology, which was like what does the IRS need that for? So, first part of what we hope will be legislation that we can have broad support on, that the chairman and both Republicans and Democrats can support, is tell us what is going on now.

And then, second, while we are trying to figure that out, while the studying and we are getting an accountability and what is all happening, let's not expand it. Let's just start there. Tell us what you are doing and don't do anything while we are trying to figure out what you are doing. And then once we get that information, then we can move from there.

That is what I hope we can start with, Madam Chair. And frankly, what we have been working with now for a year, staffs for both the majority and the minority. So, I hope—I mean, I see a number of you nodding your heads. I hope that is something, someplace that you all would be happy and would be supportive of us doing as a committee and as a Congress just to figure out what is going on.

With that, I yield to my colleague from North Dakota, if that is okay, Madam Chair, for the remainder of our time?

Chairwoman MALONEY. Sure.

Mr. ARMSTRONG. Thank you. CSI was my favorite show when I practiced criminal defense, so——

[Laughter.]

Mr. ARMSTRONG. And if this body would pass a law into effect that shut off everybody's facial recognition on their iPhones tomorrow, I think we would have a whole different kind of perspective on this from our citizens.

Identifying people quickly and easily has so many positive law enforcement and safety applications that I think it would be irresponsible to disregard this technology completely. More importantly, I think the private sector—and so my intent when I am asking these questions is not to demonize law enforcement. They will use whatever tools are available to them, and they should.

And I think we should also recognize that there are very responsible large corporations that want to get this right. And they don't want to get it right just for the bottom line, although that is helpful. They have corporate cultures as well, and more importantly, there are those of them arguing for a Federal regulatory framework.

Our job is to get it right. Our job is to ensure that we have responsible regulation that protects the privacy of all Americans. But part of doing that is recognizing that it is here, and in some way, shape, or form, it is going to continue to be here. And there are a tremendous amount of positive applications that can be used.

But there are dangers, and there are significant dangers. Because for every reason why there is a positive application for identifying people quickly, that is an invasion on everybody's privacy who is in that particular space. So, we are going to work with it. We are going to continue to use it. It is causing tremendous consumer convenience.

There are lots of different applications, but we have to be cognizant of the fact that this is a little different than a lot of other things because identity is something that can never go away once it has been identified. And right to free association and the right to do those things is fundamental in the American population. And anything that has a chilling effect on that has to be studied very, very closely.

And I agree with Mr. Jordan, in when we know how this is being used. And I also agree with Mr. Connolly. Technology will advance. Human reviews will exist. Things will happen. This will get better and better all the time.

I don't want any false positives. And I don't want any false positives based on race, age, or gender. But my number-one concern is not only those false positives, it is the actual positives—where they are doing it, how they are doing it, why they are doing it. And we have to understand that while this technology has a tremendous benefit to a lot of people, it poses real significant and unique dangers to fundamental, basic First Amendment rights, Fourth Amendment rights. And we have to continue to work forward.

I should also say this isn't the first time the Government has been behind the eight ball on these issues. We are so far behind on online piracy. We are so far behind on data collection, data sharing, and those types of issues. And one of the dangers we run into with that is by the time we get around to dealing with some of these issues, society has come to accept them. And how the next generation views privacy in a public setting is completely different than how my generation and generations above us viewed privacy in a public setting. And the world is evolving with technology, and this is going to be a part of it going forward.

So, I appreciate everybody on both sides of this issue, and I really appreciate the fact that we had this hearing today. With that, I yield back.

Chairwoman MALONEY. I thank all of the panelists and all of my colleagues today for participating in this very important hearing. We have another member, Mr. DeSaulnier is on his way, and he has been misidentified. He is a member of the committee but is at another committee. He is rushing back to share his experiences with us, and I want to allow him to give the information that he has on this issue personally.

But I do want to say that one of the things that came out of the hearing is that it really is not ready for primetime, and it can be used in many positive ways. But it can also, as many witnesses pointed out, Ms. Whittaker even showed a case allegedly where a person was innocent yet put into jail based on false information of his identity, which certainly needs to be investigated. But it can be used for positive ways, but also severely impact the civil rights and liberties of individuals.

At this point, I would like to recognize my colleague from the great state of California, that he finish his questions and his statement, because he was misidentified. He was one of the 28 that the American Civil Liberties Union showed was misidentified. So, I recognize my colleague now.

Mr. DESAULNIER. Thank you, Madam Chair.

I did have a constituent at a town hall say that in my case it was actually a step up from being a Member of Congress to being a criminal. You know, I was quite offended on behalf of all of us that somebody would——

[Laughter.]

Mr. DESAULNIER. Well, I really want to thank the chair and the ranking member for having this meeting.

It is really important, being from the Bay Area, having had a relationship with a lot of these tech companies, and having that relationship strained recently. And the benefit that this technology could give us, but the overmarketing of the benefit and the lack of social responsibility, as Mr. Gomez said.

In the past, I had a privacy bill in the legislature that was killed, and it basically came from a district attorney in northern California, who told me about a serial rapist who was getting his victims' information from third-party data that he was paying for, and we provided an opt-out. It was killed fairly dramatically in the first committee in the Assembly after I was able to get it out of the Senate. I tried to get Mr. Gomez to help me in those days.

So, in that context, if I had a dime for every time one of these companies told me when I asked a reasonable question that I was inhibiting innovation, I would be a wealthy person. And I appreciate the work you do, but in the context of facial recognition and what is a meaningful sort of reflection, I have said this to this committee before, that Justice Brandeis famously said, "Americans have a right to be left alone." How are you left alone in this kind of surveillance economy?

So, facial recognition, important to get it right in my personal experience, but also the overlay of all the other data accumulation. So, how do we get, Ms. Leong, first of all, what is the danger in allowing companies, when we have seen Facebook absorb a $5 billion penalty when they quite consciously—and I refer to some of my former friends in the tech company in the Bay Area as being led by a culture of self-righteous sociopaths. Where they think that it is all right to take advantage of people, and they get reinforced by the money they make, without thinking of the social consequences.

So, given that they were willing to absorb a $5 billion hit by ignoring the settlement that they agreed to, in this kind of culture, what is the danger in allowing companies like Facebook to having access to not just facial templates, but the interaction with all the other data they are collecting?

Ms. LEONG. Thank you very much for the question.

I think that demonstrates greatly the comment that was made earlier about the interrelationship between public and private uses of this technology and how those sometimes can feed off of each other in beneficial or not so beneficial ways. And your earlier comment was to the nature of our surveillance technology, I think is the underlying question, in terms of what is it that we want to accept and live with in our country based on our values, and then how does technology enable that?

I was not asked to show my identification to come into this building today, even though most buildings in Washington I would have to show it. To show up and go to a meeting, I'd have to give my I.D., but because this is a Government building, I was checked for a physical security threat with a scanner, but I was not required to identify myself to come in. I would hope that that would not change just because now it could be collected passively or I could be identified off of a video feed, that I still have the right to come into this place of government without that.

And I think that that demonstrates that we need to focus on what the things are that we are protected, which has been discussed so clearly here today in terms of our values and freedoms and liberties. And then how we don't let the technology, because it's here, because it can do certain things, or because it's even convenient that it does certain things, impinge on those in ways that we don't think through carefully and not ready to accept those compromises.

Mr. DESAULNIER. So, how do Americans be allowed to be left alone in this environment? What does affirmative consent look like?

Ms. LEONG. Well, in a commercial setting or a commercial context, the companies should not be using facial recognition technology unless a person has said they want to use it for the benefit or convenience that it provides. So, if I want to use it as a member of a limited membership retail establishment or if I want to use it to get VIP privileges at a hotel or expedite my check-in at a conference, I can choose to do that, but I would know that I was doing it. I would have to enroll in that system consciously. It's not something that could happen to me without my awareness.

Mr. DESAULNIER. OK. And who owns the data when you look at this? We have had hearings about car companies saying they own the diagnostics and the GPS. All these private sectors say they own it. Shouldn't we own that?

Ms. LEONG. Ownership of data is a very complicated topic and way to look at it because it isn't something that should be able to necessarily be sold, which is really the nature of property. But in terms of the rights to who has to use it, yes, that should be very clearly spelled out, in terms of if I've agreed to a certain amount of service in return for providing—for enrolling in a facial recognition system, I have a reasonable expectation not to have that data scraped or used for some other undisclosed purposes that I'm not aware of.

Mr. DESAULNIER. Thank you. Thank you, Madam Chair. Thank you for indulging my schedule.

Chairwoman MALONEY. Thank you so much. I am so glad you could get back.

And just in closing very briefly, I think this hearing showed that this is a wide-scale use. We don't even have a sense of how widely it is being used, yet there is very little transparency of how or why it is being used and what security measures are put in place to protect the American people from that use and their own privacy concerns.

And we also have the dual challenge not only of encouraging and promoting innovation, but also protecting the privacy and safety of the American consumer. I was very much interested in the passion on both sides of the aisle to work on this and get some accountability and reason to it. And I believe that legislation should be bipartisan. I firmly believe the best legislation is always bipartisan. And I hope to work in a very committed way with my colleagues on this side of the aisle and the other side of the aisle to coming up with common sense facial recognition legislation.

I would now like to recognize for closing Mr. Gomez, who was also misidentified and has personal experience with this. So, thank you, and thank you very, very much to all of our panelists.

Mr. GOMEZ. Thank you, Madam Chair.

First, I just want to thank all the panelists for being here. All the questions we have had, you know, we have twice as many more that we didn't even have a chance to ask. I want people to walk away understanding that this is a technology that is not going away. It is just going to get further and further integrated into our lives through the private sector and through Government. Now we have to figure out what does that mean.

At the same time, I don't want people to think that false positives are not a big deal because for the people who are falsely identified as a particular person and it changes their life, it is a big deal to them. So, when people like downplay it as like, oh, it is getting better, it is not that big of a deal, well, to that one person that goes to jail, the one person who gets pulled over, the one person that maybe doesn't make it to work on time, they lose their job, and has a ripple effect of devastation on their lives, it matters to them. And it should matter to all of us.

So, it is not one or the other because I do believe that this will get better and better and better. And we have to put the parameters on it on that use of that technology, but there is still a lot of questions that we have to do.

But Ms. Whittaker described it correctly because when I started looking into this issue, I did run into that brick wall of national security claims, plus the corporate sector saying that we have, you know, it is proprietary, this information, when it comes to our technology, and we are not going to tell you what it says, how accurate it is, who we are selling it to, who is using it.

That wall must come down. And that is what I think that we share across the political spectrum. How do we make sure that that wall comes down in a responsible way that keeps innovation going, keeps people safe, but respects their liberties and their freedom?

So, with that, I yield back. Madam Chair, thank you so much for this important hearing.

Chairwoman MALONEY. And I thank you. And I would like to thank all of our witnesses.

Without objection, all members will have five legislative days within which to submit additional written questions for the witnesses to the chair, which will be forwarded to the witnesses for their response. I ask the witnesses to please respond as promptly as you can.

This hearing is adjourned, and thank you.

[Whereupon, at 12:55 p.m., the committee was adjourned.]

○