FACIAL RECOGNITION TECHNOLOGY: PART II ENSURING TRANSPARENCY IN GOVERNMENT USE

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

JUNE 4, 2019

Serial No. 116–031

Printed for the use of the Committee on Oversight and Reform

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

U.S. GOVERNMENT PUBLISHING OFFICE
36–829 PDF WASHINGTON : 2019

COMMITTEE ON OVERSIGHT AND REFORM

ELIJAH E. CUMMINGS, Maryland, *Chairman*

CAROLYN B. MALONEY, New York
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
KATIE HILL, 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

JIM JORDAN, Ohio, *Ranking Minority Member*
JUSTIN AMASH, Michigan
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
RALPH NORMAN, South Carolina
CLAY HIGGINS, Louisiana
CHIP ROY, Texas
CAROL D. MILLER, West Virginia
MARK E. GREEN, Tennessee
KELLY ARMSTRONG, North Dakota
W. GREGORY STEUBE, Florida

DAVID RAPALLO, *Staff Director*
YVETTE BADU-NIMAKO, *Legislative Director/Counsel*
GINA KIM, *Counsel*
LAURA RUSH, *Deputy Clerk*
CHRISTOPHER HIXON, *Minority Staff Director*

CONTACT NUMBER: 202-225-5051

C O N T E N T S

INDEX OF DOCUMENTS

The documents entered into the record during this hearing are listed below, and are available at: https://docs.house.gov.

FACIAL RECOGNITION TECHNOLOGY: PART II
ENSURING TRANSPARENCY IN GOVERNMENT USE

Tuesday, June 4, 2019

HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND REFORM
WASHINGTON, D.C.

The committee met, pursuant to notice, at 9:59 a.m., in room 2154, Rayburn House Office Building, Hon. Elijah Cummings (chairman of the committee) presiding.

Present: Representatives Cummings, Maloney, Norton, Clay, Lynch, Connolly, Krishnamoorthi, Raskin, Rouda, Hill, Sarbanes, Welch, Speier, Kelly, DeSaulnier, Lawrence, Khanna, Gomez, Ocasio-Cortez, Pressley, Tlaib, Jordan, Amash, Gosar, Massie, Meadows, Hice, Grothman, Cloud, Higgins, Roy, Miller, Armstrong, and Steube.

Chairman CUMMINGS. The committee will come to order.

Without objection, the Chair is authorized to declare a recess of the committee at any time.

This is our second hearing on facial recognition technology.

I now recognize myself for five minutes to make an opening statement.

Today, the committee is holding our second hearing on the use of facial recognition technology, and we will be examining the use of this technology by law enforcement agencies across the Federal Government.

We had a broad survey of a full range of issues raised by technology. We heard from a number of experts about the benefits and the dangers of this technology across government and the entire private sector.

The stark conclusion after our last hearing was that this technology is evolving extremely rapidly without any real safeguards. Whether we are talking about commercial use or government use, there are real concerns about the risks that this technology poses to our civil rights and liberties and our right to privacy.

The other conclusion from our last hearing was that these concerns are indeed bipartisan. As we saw at our last hearing, among conservatives and liberals, Republicans and Democrats, there is wide agreement that we should be conducting oversight of this issue to develop commonsense, concrete proposals in this area. And I truly appreciate the Ranking Member's commitment to working together on this issue again in a bipartisan way.

Today, we will focus on the use of facial recognition technology by our government. Our committee has broad jurisdiction over all government agencies, so we are uniquely situated to review how different agencies are using this technology on the American people.

For example, today we will hear from the Federal Bureau of Investigation. In April, the Government Accountability Office sent a letter to the Department of Justice with open recommendations on the FBI's use of facial recognition technology. As that letter stated, the FBI had not implemented these recommendations despite the fact that GAO initially made them three years ago.

We will also hear from GAO, not only on the importance of these recommendations which focus on transparency and accuracy, but also on the dangers associated with failing to implement them.

We will also hear from the Transportation Security Administration, which has launched pilot programs in U.S. airports that subject American citizens to a facial recognition system.

Finally, we will hear from the National Institute of Standards and Technology, or NIST. NIST has been the standard bearer for biometric accuracy for the past 20 years. NIST will discuss the state of the technology, the rapid advancement of this technology, the accuracy challenges this technology still faces, and future plans for testing and monitoring progress.

Hearing from all of these relevant actors and building this record of information is important as we begin to stress the use of facial recognition technology by both government and private actors and potentially develop legislative solutions.

We will continue to hear from additional stakeholders through our subcommittees, each of which is tasked with a specialized focus, such as safeguarding civil rights and liberties, protecting consumers, examining our government's acquisition of this technology, and reviewing national security concerns.

I anxiously look forward to hearing from all of our witnesses today.

And now, with that, I recognize the distinguished Ranking Member of our committee, Mr. Jordan, for his opening statement.

Mr. JORDAN. Mr. Chairman, thank you. I mean it; thank you for this hearing. We fight a lot on this committee, and I think we may have a little vigorous debate tomorrow morning, but today is a subject matter where we have a lot of agreement and a lot of common ground. So I genuinely appreciate the Chairman's willingness to have a second hearing on this important subject.

Two weeks ago, we learned some important things. Facial recognition technology, there are all kinds of mistakes made when it is implemented. Those mistakes disproportionately impact African Americans. There are First Amendment and Fourth Amendment concerns when it is used by the FBI and the Federal Government. There are due process concerns when it is used by the FBI and the Federal Government.

We learned that over 20 states, 20 states, have given their Bureau of Motor Vehicles the driver's license data base. They have just given access to that to the FBI. No individual signed off on that when they renewed their driver's license or got their driver's license. They didn't sign any waiver saying, oh, it is okay to turn

my information, my photo over to the FBI. No elected officials voted to allow that to happen, no state assemblies, no general assemblies, no bills, no Governor signing something, passing a bill saying it is okay for the FBI to have this information.

And now we learn that when GAO did their investigation and study into how the FBI implemented this, there were all kinds of mistakes the FBI made in how it was implemented. I think five recommendations that the GAO said you are supposed to follow the FBI didn't follow. And it has been three years for some of those that they still haven't corrected and fixed those concerns that GAO raised with the implementation of facial recognition technology.

And all this happens, all this happens in a country with 50 million surveillance cameras.

So this is an important subject. And again, I appreciate the Chairman's willingness to have a second hearing and willingness to work together in a bipartisan fashion to figure out what we can do to safeguard American citizens' First Amendment and Fourth Amendment and due process rights as we go forward.

Chairman CUMMINGS. Thank you very much.

I now want to welcome our witnesses.

Ms. Kimberly J. Del Greco is the Deputy Assistant Director of Criminal Justice Information Services at the Federal Bureau of Investigation.

Dr. Gretta Goodwin is the Director of Homeland Security and Justice at the U.S. Government Accountability Office.

Dr. Charles Romine is the Director of the Information Technology Laboratory at the National Institute of Standards and Technology.

Mr. Austin Gould is the Assistant Administrator of Requirements and Capabilities Analysis at the Transportation Security Administration.

If you would please stand and raise your right hand, I will swear you all 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?

Let the record show that the witnesses answered in the affirmative.

Thank you very much. You may be seated.

The microphones are very sensitive, so please speak directly into them. Make sure they are on when you speak, please.

Without objection, your written statements will be made a part of the official record of this committee.

With that, Director Del Greco, you are now recognized to give your statement for five minutes.,

STATEMENT OF KIMBERLY J. DEL GRECO, DEPUTY ASSISTANT DIRECTOR, CRIMINAL JUSTICE INFORMATION SERVICES, FEDERAL BUREAU OF INVESTIGATION

Ms. DEL GRECO. Thank you, Chairman Cummings and Ranking Member Jordan, and the members of the committee. My name is Kimberly Del Greco. I am the Deputy Assistant Director leading the Information Services Branch with the FBI's Criminal Justice Information Services Division. Thank you for the opportunity to ap-

pear before the committee. I am testifying today regarding the FBI's use of facial recognition for law enforcement purposes.

It is crucial that authorized members of law enforcement and national security communities have access to today's biometric technologies to investigate, identify, apprehend, and prosecute terrorists and criminals. The FBI's Next-Generation Identification, or NGI system, which includes facial recognition, aids in our ability to solve crimes across the country. Facial recognition is an investigative tool that can greatly enhance law enforcement capabilities and protect public safety.

At the FBI, trust is crucial. Protecting the privacy and civil liberties of the American people is part of our culture. This is why, when the FBI developed its facial recognition technologies, it also pioneered a set of best practices to effectively deploy these technologies for public safety in keeping with the law and without interfering with our fundamental rights.

The FBI has two separate programs using facial recognition technology. They are the FBI's Interstate Photo System, or IPS, and the FBI's Facial Analysis Comparison and Evaluation, or FACE Services Unit.

Specifically, the NGI-IPS allows authorized law enforcement agencies the ability to use investigative tools of facial recognition by searching criminal mug shots. Law enforcement has performed photo line-ups for decades. While this practice is not new, the efficiency of such searches has significantly improved using automated facial recognition.

The FBI's policies and procedures emphasize that photo candidates returned are not to be considered positive identification, that the searches of photos will only result in a ranked listing of candidates. The FBI requires users of the NGI-IPS to follow the NGI Implementation Guide and the Facial Identification Scientific Working Group Standards for performing facial recognition comparisons. The policy places legal, training, and security requirements on law enforcement users of the NGI-IPS, including a prohibition against submitting probe photos that were obtained without respect to the First and/or Fourth Amendments.

Photos in the NGI-IPS repository are solely criminal mug shots acquired by law enforcement partners with criminal fingerprints associated with an arrest. The FBI FACE Services Unit provides investigative lead support to FBI offices, operational divisions, and legal attaches by using trained FACE examiners to compare FACE images of persons associated with open assessments or active investigations against facial images available in state and Federal facial recognition systems through established agreements with state and Federal authorities.

The FACE Services Unit only searches probe photos that have been collected pursuant to the Attorney General guidelines as part of an authorized FBI investigation, and they are not retained. This service does not provide positive identification but rather an investigative lead.

Since the GAO review and the last oversight hearing in 2017, the FBI has taken significant steps to advance the FBI's facial recognition technology. At the end of 2017, the FBI validated the accuracy rate at all list sizes. In early 2018, the FBI required law enforce-

ment users to have completed facial recognition training consistent with the FACE standards prior to conducting facial recognition searches in the NGI-IPS. Additionally, the FBI collaborated with NIST to perform the facial recognition vendor test and determined a most viable option to upgrade its current NGI-IPS algorithm. The algorithm chosen boasted an accuracy rate of 99.12 percent. Leveraging the NIST results, the FBI is implementing the upgraded facial recognition algorithm.

I would like to thank the men and women of the FBI for their unwavering commitment. I am proud to be working alongside so many mission-focused staff, protecting the country against horrific crimes.

I also want to thank the members of this committee for their engagement on this issue on behalf of the American people and our law enforcement partners.

Thank you.

Chairman CUMMINGS. Thank you very much.

Dr. Goodwin?

STATEMENT OF GRETTA L. GOODWIN, DIRECTOR, HOMELAND SECURITY AND JUSTICE, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. GOODWIN. Chairman Cummings, Ranking Member Jordan, and members of the committee, I am pleased to be here today to discuss GAO's work on the FBI's use of face recognition technology.

Over the past few decades, this technology has advanced rather quickly, and it now has wide-ranging usage, from accessing a smart phone to social media, and to helping law enforcement in criminal investigations.

However, questions exist regarding the accuracy of the technology, the transparency in its usage, and the protection of privacy and civil liberties when that technology is used to identify people based on certain characteristics.

Today I will discuss the extent to which the FBI has assured adherence to laws and policies related to privacy and transparency regarding its use of face recognition technology, as well as whether the FBI has ensured its face recognition capabilities are sufficiently accurate.

I also will provide updates on the priority recommendations that GAO issued in April of this year regarding this technology.

In our May 2016 report, we noted that two legally required documents—the Privacy Impact Assessment, otherwise known as the PIA, and the Systems of Records Notice, otherwise known as the SORN—were not being published in a timely manner. These documents are vitally important for privacy and transparency, because the PIA analyzes how personal information is collected, stored, shared, and managed, while the SORN informs the public about the very existence of the systems and the types of data being collected, among other things.

DOJ has taken actions to expedite the development process of the PIAs, but it has yet to update the process for issuing the SORNs.

We also reported on accuracy concerns about FBI's face recognition capabilities. Specifically, we found that the FBI conducted lim-

ited assessments of the accuracy of the face recognition searches before they accepted and deployed the technology. For example, the face recognition system generates a list of the requested number of photos. The FBI only assessed accuracy when users requested a list of 50 possible matches. It did not test smaller list sizes, which might have yielded different results.

Additionally, these tests did not specify how often incorrect matches were returned. Knowing all of this, the FBI still deployed the technology.

The FBI often uses face recognition systems operated by 21 state and two Federal external partners to enhance its criminal investigations. We reported that the FBI had not assessed the accuracy of these external systems. As a result, they cannot know how accurate these systems are, yet the FBI keeps using them.

Moreover, we found that the FBI did not conduct regular reviews to determine whether the searches were meeting users' needs. We made recommendations to address all of these accuracy concerns. DOJ has yet to implement these regs.

As you are aware, in April of this year we issued our annual Priority Recommendations Report which provided an overall status of DOJ's open recommendations and outlined those that GAO believes should be given high priority. This report included six recommendations related to face recognition. As of today, five of those six remain open.

The use of face recognition technology raises potential concerns about both the effectiveness of the technology in aiding law enforcement and the protection of privacy and individual civil liberties. This technology is not going away, and it is only going to grow. So it will be important that DOJ take steps to ensure the transparency of the systems so that the public is kept informed about how personal information is being used and protected; that the implementation of the technology protects individuals' privacy; and that the technology and systems used are accurate and are being used appropriately.

Chairman Cummings, Ranking Member Jordan, and members of the committee, this concludes my remarks. I am happy to answer any questions you have.

Chairman CUMMINGS. Thank you very much.

Dr. Romine?

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

Mr. ROMINE. Chairman Cummings, 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, or NIST. Thank you for the opportunity to appear before you today to discuss NIST's role in standards and testing for facial recognition technologies.

In the area of biometrics, NIST has been working with the public and private sectors since the 1960's. NIST's work improves the accuracy, quality, usability, interoperability, and consistency of iden-

tity 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. NIST leads national and international consensus standards activities in biometrics such as facial recognition technology, but also in cryptography, electronic credentialing, secure network protocols, software and systems reliability, and security conformance testing, all essential to accelerate the development and deployment of information and communication systems that are interoperable, reliable, secure, and usable.

NIST biometric evaluations advance the technology by identifying and reporting gaps and limitations of current biometric recognition technologies. NIST evaluations advance measurement science by providing a scientific basis for what to measure and how to measure. NIST evaluations also facilitate development of consensus-based standards by providing quantitative data for development of scientifically sound, fit-for-purpose standards.

NIST conducted the Face Recognition Grand Challenge and multiple biometric grand challenge programs to challenge the facial recognition community to break new ground, solving research problems on the biometric frontier. Since 2000, NIST's Face Recognition Vendor Testing Program, or FRVT, has assessed capabilities of facial recognition algorithms for one-to-many identification and one-to-one verification. NIST expanded its facial recognition evaluations in 2017. NIST broadened the scope of its work in this area to understand the upper limits of human capabilities to recognize faces and how these capabilities fit into facial recognition applications.

Historically and currently, NIST biometrics research has assisted the Federal Bureau of Investigation, the FBI, and Department of Homeland Security, or DHS. NIST's research was used by DHS in its transition to ten prints for the former US-VISIT program. NIST is currently working with FBI and DHS to analyze face recognition capabilities, including performance impacts due to image quality and demographics, and provide recommendations regarding match algorithms, optimal thresholds, and match gallery creation.

NIST's Face Recognition Vendor Testing Program was established in 2000 to provide independent evaluations of both prototype and commercially available facial recognition algorithms. Significant progress has been made in algorithm improvements since the program was created.

NIST is researching how to measure the accuracy of forensic examiners matching identity across different photographs. The study measures face identification accuracy for an international group of professional forensic face examiners working under circumstances approximating real-world case work. The findings, published in the Proceedings of the National Academy of Sciences, showed that examiners and other human face specialists, including forensically trained facial reviewers and untrained super-recognizers, were more accurate than the control groups on a challenging test of face identification. It also presented data comparing state-of-the-art facial recognition algorithms with the best human face identifiers.

Optimal face identification was achieved only when humans and machines collaborated.

As with all areas, for face recognition, rigorous testing and standards development can increase productivity and efficiency in government and industry, expand innovation and competition, broaden opportunities for international trade, conserve resources, provide consumer benefit and choice, improve the environment, and promote health and safety.

Thank you for the opportunity to testify on NIST activities in facial recognition, and I would be happy to answer any questions you may have.

Chairman CUMMINGS. Thank you very much.

Mr. Gould?

STATEMENT OF AUSTIN GOULD, ASSISTANT ADMINISTRATOR, REQUIREMENTS AND CAPABILITIES ANALYSIS, TRANSPORTATION SECURITY ADMINISTRATION

Mr. GOULD. Good morning, Chairman Cummings, Ranking Member Jordan, and distinguished members of the committee. Thank you for inviting me before you to discuss the future of biometric identity management at the Transportation Security Administration.

I am Austin Gould, the Assistant Administrator for Requirements and Capability Analysis at TSA. I would like to thank the committee for working with TSA as we continue to improve the security of transportation systems, and particularly for your support of our officers at airports nationwide.

TSA's establishment in 2001 charged the agency with providing transportation system security. A key component to performing this mission is positively identifying passengers who are boarding aircraft and directing them to the appropriate level of physical screening. This primarily occurs when passengers enter a checkpoint and present themselves to a security officer. Since its inception, TSA has strived to carry out that role as effectively and efficiently as possible using available technology.

Recognizing the need to positively identify passengers in an era where fraudulent means of identification are becoming more sophisticated and prevalent, TSA has consistently sought new processes and technologies to improve performance while protecting passengers' privacy. To that end, TSA's 2018 Biometrics Roadmap identifies the steps that the agency is taking to test and potentially expand biometric identification capability at TSA checkpoints, which we believe can both enhance security and improve passenger experience.

The Roadmap has four major goals: partner with Customs and Border Protection on biometrics for international travelers; operationalize biometrics for TSA pre-check passengers; potentially expand biometrics for additional domestic travelers; and develop the infrastructure to support these biometric efforts.

Consistent with the Biometrics Roadmap, TSA has conducted pilots that use facial biometrics to verify identity at certain airports. These pilots are of limited scope and duration and are being used to evaluate the applicability of biometric technology for TSA operations. The pilots to date have been executed in conjunction with

Customs and Border Protection. Each pilot has been supported by a privacy impact assessment, and passengers always have the opportunity to not participate. In these cases, standard manual identification process is used.

I have observed the pilot currently underway in Terminal F in Atlanta for international passengers. Of note, virtually every passenger chose to use the biometric identification process. The facial capture camera used for this pilot was in active mode, meaning that it only captured a facial image after the passenger was in position and the officer activated it. The match rate is extremely high, and passengers moved rapidly through the checkpoint.

In that regard, biometrics represents a unique opportunity for TSA. This capability can increase security effectiveness for the entire system by using biometric identification while also increasing throughput at the checkpoint and enhancing the passengers' experience. The ability to increase throughput while providing more effective passenger identification will be extremely beneficial as we continue to see increasing passenger volumes, which are growing at a rate of approximately four percent annually. In fact, we experienced our busiest travel day ever on 24 May, the Friday of Memorial Day weekend, when we screened approximately 2.8 million passengers and crew.

TSA is committed to addressing accuracy, privacy, and cybersecurity concerns associated with biometrics capture and matching. In that regard and pursuant to Section 1919 of the TSA Modernization Act, DHS will submit a report that includes assessments by TSA and CDP that were developed with the support of the DHS Science and Technology Directorate. This report will address accuracy, error rates, and privacy issues associated with biometric identification.

Looking ahead, TSA plans to continue to build upon the success of past pilots by conducting additional ones at select locations and limited durations to refine requirements for biometric implementation at TSA checkpoints. These pilots will be supported by privacy impact assessments, clearly identified by airport signage, and passengers will always have the opportunity to choose not to participate.

To close, TSA is in the process of a systematic assessment of the applicability of biometric identification at our checkpoints. This identification process will enhance aviation security while also increasing passenger throughput and making air travel a more enjoyable experience. TSA's system will be used for passenger identification and to determine the appropriate level of screening only. It will not be used for law enforcement purposes. And as always, passengers will have the opportunity to not participate.

Thank you for the opportunity to address this important issue before the committee, and I look forward to answering your questions.

Chairman CUMMINGS. I now recognize myself.

Ms. Del Greco, in 2017 the Government Accountability Office testified before our committee that the FBI had signed contracts with at least 16 states to be able to request searches of their photo data bases. The GAO stated that most of these systems accessed driver's

license photos, but several states also include mug shots or correction photos.

Ms. Del Greco, can you explain how the FBI decides to search a state data base versus when it searches its own system, and how this policy is determined?

Ms. DEL GRECO. I would be happy to explain that. At the FBI we have a service called FACE Services Unit. They process background checks and process facial recognition searches of the state DMV photos. They do this in accordance with the Attorney General guidelines. An FBI field office has to have an open assessment or an active investigation. They submit the probe photo to the FBI FACE Services Unit. We launch the search to the state. The state runs the search for the FBI and provides a candidate list back.

With regard to the NGI-IPS, the Interstate Photo System, the FACE Services Unit will utilize that repository, as well as the DMV photos. However, state and local and Federal law enforcement agencies only have access to the NGI Interstate Photo System. These are the FBI mug shots that are associated with a ten print criminal card associated with a criminal arrest record.

Chairman CUMMINGS. Well, do individuals who consent to having their faces in the non-criminal data bases also consent to having their faces searched by the FBI for criminal investigations? For example, when applying for a driver's license, does someone consent at the DMV to being in a data base searchable by the FBI?

Ms. DEL GRECO. The FBI worked diligently with the state representatives in each of the states that we have MOUs. We did so under the state's authority to allow photos to be used for criminal investigations. We also abided by the Federal Driver's License Privacy Protection Act, and we consider that a very important process for us to access those photos to assist the state and local law enforcement and our Federal agencies.

Chairman CUMMINGS. Well, you just said state authority allows you to do this. One question that our Ranking Member has been asking over and over again is do you know whether in these states, do any elected officials have anything to do with these decisions? In other words, where is that authority coming from? We are trying to figure out, with something affecting so many citizens, whether elected officials have anything to do with it. Do you know?

Ms. DEL GRECO. I do. Only in one state, the state of Illinois, did an elected official sign the MOU. In the other states, they were done with the state representatives. This is state law that is established at the state level prior to facial recognition and our program getting started. We are just leveraging that state law. That state law is already in place. We did work with the Office of General Counsel at the FBI, and at the attorney level at the state level.

Chairman CUMMINGS. Well, if it was prior to facial recognition coming into existence, I am just wondering, do you think that whatever laws you are referring to anticipated something like facial recognition?

Ms. DEL GRECO. It is my understanding that the states established those laws because of fraud and abuse of driver's licenses, and we are just reviewing each of the state laws and working with the representatives in those states to ensure that we can leverage that for criminal investigation.

Chairman CUMMINGS. So when you say "leverage," I guess you are saying that there were laws that were out there. These laws did not anticipate something like facial recognition, and now the FBI has decided that it would basically take advantage of those laws; is that right? Is that a fair statement?

Ms. DEL GRECO. The Federal Driver's License Privacy Protection Act, it allows the state to disclose personal information, including a photo or an image obtained in connection with a motor vehicle record, to law enforcement to carry out its official function.

Chairman CUMMINGS. Okay, I just have a few more questions. We have seen significant concern among states about providing this level of access to the FBI. For example, during our May 22 hearing, we learned that Vermont suspended the FBI's use of its driver's license data base in 2017; is that correct?

Ms. DEL GRECO. I am not aware of that, sir.

Chairman CUMMINGS. Well, it is accurate.

Ms. Del Greco, how many states have provided this level of direct access to the FBI?

Ms. Del GRECO. We do not have direct access. We submit a probe to the state. There's 21 states——

Chairman CUMMINGS. Twenty-one states, okay.

Ms. Del Greco. And what we did, sir, in the last two years, since the last oversight hearing, our Office of General Counsel reviewed every single MOU to ensure that it met the Federal and the state authorities.

Chairman CUMMINGS. Does the FBI have plans to increase the number of states that provide the FBI with access to its data bases?

Ms. DEL GRECO. That would be up to the states, sir. We have reached out to all the states, but it is up to them and their state authorities and state representatives if they want their data used. It is optional for them.

Chairman CUMMINGS. When states agree to provide this level of access to the FBI data base, are they aware of the FBI policies when searching their systems and any changes that are made to these policies?

Ms. DEL GRECO. It is made extremely clear to each of the states how the information will be used, the retention. We purge all photos coming back to us from the state. We ask that the state purge all of the probe photos that we send them. There is——

Chairman CUMMINGS. How do you make them aware?

Ms. DEL GRECO. We have active discussions, and then it is in the MOU, sir.

Chairman CUMMINGS. Is the FBI undergoing any current negotiations to expand the information available for FBI face services, photo services? If so, can you please describe these negotiations?

Ms. DEL GRECO. I am not aware of any current negotiations right now, sir.

Chairman CUMMINGS. Now, finally, we also heard reports that the FBI can search photo data bases of other agencies, including the Department of state. Are there any limits to this access?

Ms. DEL GRECO. The searches of the state Department's photo is in accordance with an active FBI investigation and are only done under the Attorney General guidelines followed by the FBI.

Chairman CUMMINGS. And can the FBI perform a face recognition search for any American with a passport?

Ms. DEL GRECO. For an open assessment or an active investigation, only by the FBI, sir.

Chairman CUMMINGS. All right. I now recognize Mr. Gosar.

Mr. GOSAR. I thank the Chairman, and thanks for bringing this important issue to the forefront.

Now, I know we don't have Border Patrol here and their use of facial recognition to meet the congressional mandate for biometrics, and I know that they have had some success. Also, I am from the state of Arizona, and our Department of Transportation uses this technology to combat fraudulent driver's license applications.

Mr. Gould and Ms. Del Greco, can you give us a little bit more information and details on some of the successes with partners that you have been working with?

Ms. Del Greco?

Ms. DEL GRECO. The successes that we have had, the majority are with state and local law enforcement. The FBI is not a positive identification. It provides investigative leads out to law enforcement and to our FBI field offices. Some of those successes are assisting with the capture of a terrorist in Boston, assisting with putting the pieces together to identify where a pedophile is that was trying to avoid law enforcement for 20 years, and also assisting in identifying a person that was on the 10 Most Wanted list for homicide.

Mr. GOSAR. Mr. Gould?

Mr. GOULD. Sir, our greatest success in terms of partnering has been with Customs and Border Protection. We leverage their travel and verification system for biometrics identification at our checkpoints. As I said in my opening statement, we are doing this solely on a pilot basis, but so far the results have indicated a very high positive match rate, and it has increased through our checkpoints.

Mr. GOSAR. Mr. Romine, at our last hearing we heard some disturbing facts about accuracy of facial recognition. Can you give us some idea about, from what you see, are we going to be able to be much more accurate in that application?

Mr. ROMINE. Yes, sir. The most recent testing that we have conducted demonstrates significant improvement over previous tests. We conducted tests in 2010 and 2014 and demonstrated certain limitations associated with facial recognition accuracy. The most recent test results will be published this month for the FRVT one-to-many evaluation that is being readied, but the results so far suggest substantial increases in accuracy across the board.

Mr. GOSAR. So what sort of accuracy rates are you finding in the different algorithms' ability to match an image against a larger gallery of images?

Mr. ROMINE. The accuracy rates that we are seeing, we have many different participants who have submitted algorithms, approximately 70 participants in our testing. The best algorithms are performing at a rate of approximately 99.7 in terms of accuracy. There is still a wide variety or a wide variance across the number of algorithms, so this is certainly not commoditized yet. Some of the participants fared significantly poorer than that. But the best algorithms are in the 99 to 99.7 category.

Mr. GOSAR. So are there algorithms that you tested that you would recommend for law enforcement?

Mr. ROMINE. We don't make recommendations about specific algorithms. We provide the data necessary for making informed decisions about how an algorithm will perform in the field. So for law enforcement, for example, accuracy rates are one important aspect that needs to be considered, but there are other aspects that have to be taken into consideration for procurement or acquisition of such technology.

Mr. GOSAR. So going back to the development of algorithms, really the bias can be built into those that are manufacturing or building the algorithm; isn't that true?

Mr. ROMINE. It is true that the algorithms, depending on the way that they have been developed, can have biases associated with them. In many cases the improvement that we see in the performance of these algorithms, the dramatic improvement, comes from a transition that the vendor community and participant community have made to deep-learning algorithms, these machine-learning algorithms that are what has made the difference.

Now, let me be clear. We test these or we evaluate these as black boxes. So my assertion there is from discussions that we have had with vendors and not from examination of the algorithms themselves. And the training of those algorithms determines the level of bias that may exist within the algorithms themselves.

Mr. GOSAR. I thank the Chairman.

Chairman CUMMINGS. Thank you very much.

Mr. Lynch?

Mr. LYNCH. Thank you, Mr. Chairman. I want to thank you for holding a second hearing on facial recognition. I thank the Ranking Member as well. It is good to have bipartisan interest on this issue.

Ms. Del Greco, I certainly understand the dynamic at play when there is an active FBI investigation ongoing and you are reviewing mug shots of known criminals.

But, Mr. Gould, according to the Biometrics Roadmap released by TSA in September 2018, TSA seeks to expand the use of facial recognition technology to, quote, "the general flying public" in specific locations, but the general flying public. And TSA envisions the use of technology upon domestic flights as well as international, which would capture the faces of mostly American citizens.

I am just curious, going back to the Chairman's original question, what is the legal basis? I am not talking about a situation with the FBI where you might have—you hopefully would have probable cause. Where does the TSA find its justification, its legal justification for capturing the facial identity of the flying public?

Mr. GOULD. Yes, sir. In accordance with the Aviation Transportation Security Act of 2001, TSA is charged with positively identifying passengers who are boarding aircraft.

Mr. LYNCH. Right. Let me just stop you right there. So, we all fly, at least a couple of times a week.

Mr. GOULD. Yes, sir.

Mr. LYNCH. So now you have to have a certified license. You can't go with the old version that your state had. Now we have much more accurate licenses. We surrender that. Oftentimes in the airport in the boarding process, you have to show it a couple of

times. You have a ticketing issue there. So, you are doing that right now.

Mr. GOULD. Yes, sir.

Mr. LYNCH. You have been doing that for a long, long time.

Mr. GOULD. Manually. Yes, sir.

Mr. LYNCH. Right, right. So now you are saying that you are going to do these pilot programs and you are just going to herd people—now, you are saying voluntarily, but I could imagine, like you have done with pre-check, you can either agree to surrender your right to anonymity and wait in the long line, or you can give up your Fourth Amendment rights and go in the quick line. Is that the dynamic that is going on here?

Mr. GOULD. Sir, with respect to expanding to the general traveling public, we anticipate using—we have not tested this yet—a one-to-one matching capability at the checkpoint. You produce your credential, you stick it in a machine, and the machine identifies whether or not your image, which is captured by the camera, matches the image that is embedded in the credential, and it returns a match result. That will then allow you to proceed through the checkpoint. Should you decide not to participate in that program, we will always have the option to do that process manually.

Mr. LYNCH. Right. But to match, you have to have that data on board in the technology to begin with, to match something with; right?

Mr. GOULD. Sir, that data is embedded in your credential. So the photograph is on your driver's license, for example. There is a digital recording of that image in the credential, and when your picture is captured by the camera, it is matched to the photograph on the credential. It does not depart the checkpoint for any data base search or anything like that.

Mr. LYNCH. Okay.

Mr. GOULD. That is the one-to-one identification that we intend to use for the broader traveling public.

Mr. LYNCH. And that is it? You don't anticipate using a data base or collecting a data base of information within TSA with which to identify passengers?

Mr. GOULD. Sir, for international travelers who have a passport photo on record, and for TSA pre-check passengers who also provide a passport photo, we will match them to a gallery. But for the general traveling public that does not participate in those programs and merely has a credential, that match——

Mr. LYNCH. What is the size of the gallery? What do you anticipate? If anybody engages in international travel, are they going to be in that, or are they foreign nationals who travel to the U.S.?

Mr. GOULD. Sir, the gallery that we use right now with TVS includes anyone who is traveling internationally and who has a photo on record.

Mr. LYNCH. Well, here is the problem. We had a problem with OPM where we had 20 million individuals, their personal information, Social Security numbers, everything that they submitted on Federal documents to OPM was stolen by, we think, the Chinese. I am just curious and concerned that we don't have a great track record here in protecting people's personal information.

Mr. GOULD. Yes, sir. And the cybersecurity rules associated with this program is something that we take very, very seriously.

Mr. LYNCH. I hope so.

My time has expired. I yield back.

Chairman CUMMINGS. Thank you very much.

Mr. Higgins?

Mr. HIGGINS. Thank you, Mr. Chairman.

Ladies and gentlemen, thank you for appearing before the committee today.

Mr. Chairman, I ask unanimous consent to enter into the record a document from the security industry association. It is the Association for Cybersecurity Providers, just a general knowledge document. I ask unanimous consent.

Chairman CUMMINGS. Without objection, so ordered.

Mr. HIGGINS. During this emerging technology era of digital technologies, I think it is important that we refer to technologies that we have had existing for quite some time. In 2005, as a police officer, we had in the city that I patrolled, we had access to a camera, a series of cameras that were disguised as transformers on electric poles. When we had large numbers of complaints on crimes in portions of the city, and the citizenry themselves would want these crimes solved and investigated, we would have the linemen for the electric company install this camera, and we solved many crimes, and crimes would go down. This was 15 years ago.

We have license plate readers right now. Madam, gentlemen, I am sure you are quite familiar with license plate readers. We use them from sea to shining sea. If your vehicle is on a public road, it is subject to a license plate reader. In fact, these cameras are not available to just law enforcement but any citizen who chooses to invest the treasure—they are quite expensive—can read the license plate, and it is cross-referenced to the DMV. They now know exactly what vehicle passed in front of that camera. These cameras have been used to successfully investigate and solve crimes, some of them heinous crimes, crimes numbering in the scores of thousands across the country.

I have in my home 11 smart cameras. These cameras are connected to software, high-resolution digital cameras. The software interprets the imagery to determine if it is a familiar person or not. If it is a familiar person that the cameras have learned is a constant visitor to my home—myself, my wife, my son, et cetera—then there is no alert sent to the security company. If it is not a familiar person, then a human being receives a prompt and looks at that camera feed to my home.

These are technologies that exist that we all have. Everyone here wants to protect Fourth Amendment rights and privacy rights of American citizens. None of us want our constitutional protections violated. But the fact is this emerging technology of facial recognition is coming, and it is reflecting just the advancement of our digital technologies that we have already employed across the country and deployed in public areas, including airports.

Ms. Del Greco, like any technology, there is a chance for abuse. Would you concur?

Ms. DEL GRECO. We feel at the FBI that following policies and procedures is extremely important.

Mr. HIGGINS. Thank you. And these are human beings following policies and procedures; correct?

Ms. DEL GRECO. We require all authorized state and local law enforcement entities to adhere to the required training and——

Mr. HIGGINS. Thank you, ma'am. So the technologies that we are viewing, these cameras don't make arrests, do they? They just add to the data of a case file or to the strength of an investigation, and a human being, an investigator must follow up on that and determine if you have probable cause for arrest. Is that correct?

Ms. DEL GRECO. Our system doesn't capture real time. A probe photo has to be submitted to the NGI-IPS by law enforcement, and they have to have authority to access our system for a law enforcement purpose.

Mr. HIGGINS. Well, the concern of this committee, as it should be, is the potential abuse of this technology. And I believe the point that we should clarify in my remaining 10 seconds here is that human beings are ultimately in control of the investigative effort, and that the technology that is viewed is part of a much larger totality of circumstances in any criminal investigation. Would you concur with that, ma'am?

Ms. DEL GRECO. For the FBI, we are very strict on the use of our system and the authorities that are provided to those law enforcement entities.

Mr. HIGGINS. Thank you, Madam.

Mr. Chairman, my time has expired.

Chairman CUMMINGS. What do you mean by "strict"? What does that mean?

Ms. DEL GRECO. Since the last hearing in 2017, the FBI—we take this very seriously, sir. We went out to our advisory policy board made up of over 100 state, local, Federal, and tribal entities. We talked to them about the GAO findings. We talked to them about collecting photos against the First and Fourth Amendments. We require state and local and Federal and tribal entities to have training to submit a photo to the NGI-IPS. We restrict the access unless they are authorized to have it.

We also put out the NGI Policy and Implementation Guide, and we told the states they must follow the standards that were identified in the Facial Identification Scientific Working Group Standards.

Chairman CUMMINGS. Mr. Clay?

Mr. CLAY. Thank you, Mr. Chairman. I want to thank you and the Ranking Member for conducting this hearing, and the witnesses for being here.

Let me start with what the GAO recommended in May 2016, that the FBI make changes to ensure transparency of its use of facial recognition technology. In April 2019, GAO released a letter to the Department of Justice highlighting these recommendations, recommending, and I quote, "DOJ determine, number 1, privacy impact assessments; and 2, a system of records notice where not published as required, and implement corrective actions," end of quote.

DOJ did not agree with either of these recommendations, and the FBI still has not fully implemented the two open recommendations offered by GAO.

Dr. Goodwin, can you explain the importance of transparency when it comes to the FBI's use of facial recognition technology?

Ms. GOODWIN. Yes. Thank you, sir. So, as you mentioned, we made six recommendations. Three of them related to privacy, three of them related to accuracy. Only one of those has been closed and implemented. The ones we made related to privacy and accuracy focused on the privacy impact assessment, and that is a requirement under the E-Gov Act of 2002, that PIAs be conducted to help determine the privacy implications and evaluate the protections. So the DOJ has disagreed with that. We know that they are concerned about privacy and transparency, but they disagree with our recommendation.

These are legally required documents that they have to submit. So they have to submit the PIA, and they have to submit the SORN. The SORN is required under the Privacy Act, and that provides information—anytime there is a change to the system or a change to the technology, they have to make that information publicly available so that the public knows what is going on.

So we stand behind those recommendations because those speak to transparency and those speak to privacy.

Mr. CLAY. And to this day, those documents have not been made public.

Ms. GOODWIN. That is correct.

Mr. CLAY. So, Ms. Del Greco, can you explain why the FBI disagrees with these transparency-focused recommendations?

Ms. DEL GRECO. I believe DOJ disagrees with GAO's assessment of the legal requirements. The FBI did publish both the PIA and the SORN. Initial developments of the face recognition, we had privacy attorneys embedded in our process to develop the protocols and procedures, and we have submitted updates, continuing updates to the PIA and the SORN, and we have provided updates to the GAO.

Mr. CLAY. Okay. So what steps do you take to protect privacy when conducting face recognition searches?

Ms. DEL GRECO. The FBI monitors the appropriate audits with audits of the state, local, Federal, and tribal entities. We look at four system requirements. We provide outreach to our users, and to date we have not had any violations or notice from the public that they feel like their rights are violated.

Mr. CLAY. And to what extent do you share the steps you take with the public?

Ms. DEL GRECO. So those—with regard to the PIA and the SORN, those are on behalf of the Department of Justice, and I would have to take that question back to them, sir.

Mr. CLAY. I see. Would you get back to us with a response?

Ms. DEL GRECO. Yes, sir.

Mr. CLAY. You know, I am concerned that the FBI is not fully complying with this notice obligation when it comes to the use of facial recognition. Ms. Del Greco, when the FBI arrests an individual based on a lead generated by face recognition, does it notify a defendant of that fact?

Ms. DEL GRECO. So those are through FBI open assessments or active investigations, and they are done so conforming to and fol-

lowing the Attorney General guidelines, and that would be for an active FBI investigation.

Mr. CLAY. So how many times has the FBI provided notice to criminal defendants that face recognition was used in their case?

Ms. DEL GRECO. As part of a criminal investigation, I don't believe that is part of the process.

Mr. CLAY. Oh. What about when it gets to trial? When it gets through discovery they get that?

Ms. DEL GRECO. So, the FBI FACE Services Unit, and that is the department that I represent, the CJIS Division in Clarksburg, West Virginia, we provide a candidate back to the FBI field office, two or more candidates, and they make the determination whether that is a match or not, or their person of interest that they are looking for.

Mr. CLAY. So does the FBI provide other candidate matches to the defendant as part of Brady evidence or discovery?

Ms. DEL GRECO. I am not aware of any other information other than a candidate back from a search of the facial—the NGI Interstate Photo System.

Mr. CLAY. Okay. What steps are the FBI taking to ensure that its use of the technology is as transparent as possible by showing proper notification?

Ms. DEL GRECO. The FBI provides policy and procedures out to state and local entities that they must follow. They have to follow the standards that we establish, and they have to make sure that they do so in accordance with authorized law enforcement purposes.

Mr. CLAY. So how does the public know whether their face image might be subject to searches you conduct?

Ms. DEL GRECO. The law enforcement entity would have to have the authority to do so for criminal justice purposes in order to access the NGI Interstate Photo System.

Mr. CLAY. I see. All right.

My time has expired. I yield back, Mr. Chairman.

Chairman CUMMINGS. Mr. Jordan?

Mr. JORDAN. Thank you, Mr. Chairman.

Dr. Goodwin, did the FBI meet all the requirements of the E-Government law?

Ms. GOODWIN. So, as I mentioned earlier, the PIA is the E-Government——

Mr. JORDAN. Did they meet all the requirements? I was kind of looking for a yes or no. Did they meet all the requirements when they implemented——

Ms. GOODWIN. No. We still have open recommendations related to the——

Mr. JORDAN. No, I understand.

Dr. Goodwin, did the FBI publish privacy impact assessments in a timely fashion as it was supposed to when it implemented FRT in 2011?

Ms. GOODWIN. No.

Mr. JORDAN. Did the FBI file proper notice, specifically the system of record notice, in a timely fashion when it implemented facial recognition technology?

Ms. GOODWIN. No.

Mr. JORDAN. Did the FBI conduct proper testing of the Next-Generation Interstate Photo System when it implemented FRT?

Ms. GOODWIN. Proper in terms of determining its accuracy for its use?

Mr. JORDAN. Yes.

Ms. GOODWIN. No.

Mr. JORDAN. Did the FBI test the accuracy of the state systems that it interfaced with?

Ms. GOODWIN. No.

Mr. JORDAN. So, it didn't follow the law, the E-Government law, it didn't file proper privacy impact assessment notices like it was supposed to, didn't provide timely notice, didn't provide proper testing of the system it had, and didn't check the accuracy of the state system that it was going to interface with; right? Those five things they didn't do.

Ms. GOODWIN. That is correct.

Mr. JORDAN. But Ms. Del Greco said we have strict standards, you can count on us. We've got Memorandums of Understanding with the respective states to safeguard people. That is what she told us. But when they started this system, stood up this system, there were five key things they were supposed to follow that they didn't, and my understanding is they still haven't corrected all those; is that accurate?

Ms. GOODWIN. That is correct.

Mr. JORDAN. So they still haven't fixed the five things they were supposed to do when they first started.

Ms. GOODWIN. We still have five open recommendations.

Mr. JORDAN. But we are supposed to believe, don't worry, everything is just fine, and we haven't even got to the fundamentals yet. We haven't even got to the First Amendment concerns, the Fourth Amendment concerns. We are just talking about the process for implementing standing up the system.

Ms. Del Greco, you said earlier to the Chairman—I think you used the words "strict policies that we follow." Now, how are we supposed to have confidence in strict policies that you are going to follow when you didn't follow the rules when you set the thing up in the first place?

Ms. DEL GRECO. Sir, the FBI published both the PIA and the SORN. The DOJ, Department of Justice, disagrees with GAO on how they interpret the legal assessment of the PIA and SORN.

Mr. JORDAN. Do you just disagree with them in one area or all five?

Ms. DEL GRECO. I believe in the three areas of the findings for GAO.

Mr. JORDAN. You have five problems.

Ms. DEL GRECO. The accuracy was tested of the system. We disagree with GAO. And actually, since the last hearing in 2017, the FBI went back and we evaluated our current algorithm again at all list sizes, and the accuracy boasted above a 90 percentile than what we had reported initially in the hearing. We do care about the accuracy of the system and the testing.

Mr. JORDAN. Earlier you said, when the Chairman was asking some questions, you said that there are folks who signed Memorandums of Understanding between—someone at the FBI signed some

document, and someone in the 21 respective states to allow access to their data base signs these Memorandums of Understanding. Who are the people signing that document, signing away the rights of the citizens in their respective states? Who are those individuals?

Ms. DEL GRECO. Our Office of General Counsel works with the state representatives in the state that garners those authorities.

Mr. JORDAN. But not state representatives in the sense that they are elected to the General Assembly in those respective states. Some person designated by somebody to sign away—I know in Ohio—I think I said this two weeks ago—we have 11 million people in our state. My guess is 8, 9, 10 million of them drive. So someone is signing away access to those 9 million people's faces, their picture and everything else in that data base. Who is that individual?

Ms. DEL GRECO. The state authorities are public documents that anyone could get access to. We work with the appropriate state officials. We review those documents very carefully. We talk about the use of the data, and we make sure they are in accordance with our Federal Driver's License Privacy Protection Act as well.

Mr. JORDAN. Okay.

Mr. Chairman, again, I just come back to the basics. Five key things they were supposed to do when they started implementing the system, I think dating all the way back to 2011, if I read the material correctly, that they didn't follow, and yet we are supposed to believe don't worry, don't worry, everything is just fine, all this happening in an environment, as we said earlier—we learned two weeks ago an environment where there are 50 million surveillance cameras around the country.

Again, I appreciate the Chairman's willingness to have a second hearing on this and his willingness to work with the minority party in trying to figure out where we go down the road.

With that, I yield back.

Chairman CUMMINGS. What is your disagreement, by the way, with GAO? You said there is a disagreement. What is it?

Ms. DEL GRECO. With regard to privacy?

Chairman CUMMINGS. Yes.

Ms. DEL GRECO. DOJ, I understand, disagrees with the legal assessment of the PIA, the SORN, and the reporting of such. But I would have to take that specifically back to DOJ to respond.

Chairman CUMMINGS. Would you do that for us, please?

Ms. DEL GRECO. I will, sir.

Chairman CUMMINGS. Thank you very much.

Ms. Maloney?

Mrs. MALONEY. Thank you, Mr. Chairman, and thank you and the Ranking Member and all the panelists for being here on this important hearing.

I have read that facial recognition technology is susceptible to errors that can have grave ramifications for certain vulnerable populations. I have read that for some reason it is more difficult to recognize women and minorities. I would like a private meeting with members who are interested in this on why this was reported, if it was reported correctly.

But what I want to do is follow up on the Ranking Member's questions on really the scope and accountability of this program.

So, Ms. Del Greco, how many searches has the FBI run in the Next-Generation Identification Interstate Photo System to date? How many searches? Do you have that information?

Ms. DEL GRECO. I have from Fiscal Year 2017 to April 2019. There were 152,500 searches.

Mrs. MALONEY. Okay. And does the FBI track if the results of this system are useful in your investigations?

Ms. DEL GRECO. We do ask our state, local, Federal, and tribal to provide feedback on the services that we provide. To date, we have not received any negative feedback.

Mrs. MALONEY. But have they said that it has been successful? Can you get back to me in writing? It is one thing not getting any feedback. The other is, is there any proof that this system has been helpful to law enforcement in any way? Has it led to a conviction? And get it to me in writing.

How many of the FBI's searches have led to arrests and convictions? Do you have that information?

Ms. DEL GRECO. I do not.

Mrs. MALONEY. You do not. How many of the FBI's searches have led to the arrest of innocent people?

Ms. DEL GRECO. For facial recognition, the law enforcement entity must have authorized access to our system, and they must do so for——

Mrs. MALONEY. But my question was has it led to the arrest of any innocent people? Yes or no?

Ms. DEL GRECO. Not to my knowledge, ma'am.

Mrs. MALONEY. Okay. And are you tracking the number of searches that have led to arrests? You don't know anything about any innocent person being arrested?

Ms. DEL GRECO. Our system is not built for identification. We provide two or more——

Mrs. MALONEY. Okay. Maybe we should change your system, then, because we need accountability on if this system is working or not, or if it is just abusing people.

And the FBI data base contains over 600 million photos of individuals that are primarily of people who have never been convicted of a crime. And my question is why does the FBI need to gather photos of innocent people?

Ms. DEL GRECO. We do not have innocent people or citizens in our data base. We have criminal mug shot photos associated with a criminal arrest.

Mrs. MALONEY. Well, then my information that I read in the paper must be wrong. I am going to follow up with a letter for clarification, because I was told you had 600 million in your data base of innocent people.

To me it is extremely important that we know whether the use of this technology leads to any benefits for society, especially in determining whether there is a crime that this is helping to solve, or are we just weighing in on constitutional rights of people and creating constitutional risk? We cannot know this unless there is a sufficient data base for law enforcement that uses this.

So my question is what are the current reporting requirements regarding the FBI's use of facial recognition technology? Is there any oversight reporting requirements on the use of this technology?

Ms. DEL GRECO. The FBI monitors appropriate uses of our technology through audits. We have a robust triennial audit where we have——

Mrs. MALONEY. Do you have a data base that tracks whether or not this is actually working, is it helping law enforcement arrest people, is it arresting innocent people, is it keeping information on innocent people? Do you have a data base that basically tells us what this program is doing and what the benefits or penalties are to our society?

Ms. DEL GRECO. No, we do not.

Mrs. MALONEY. Well, I think you should have one, and I am going to go to work on one right now. I am very concerned about it, and the American people deserve government accountability, and I actually agree with the questioning of the minority party leadership on this, that you don't have answers on how it is working, how it was set up, what is coming out of it, whether it is hurting people, helping people. You don't even have information on whether it is aiding law enforcement in their goal for hunting down terrorists. So we need more accountability, and I yield back.

Chairman CUMMINGS. Thank you very much.

Mr. Massie?

Mr. JORDAN. Mr. Chairman——

Chairman CUMMINGS. I am sorry. Real quick, I recognize the Ranking Member for a unanimous consent request.

Mr. JORDAN. Unanimous consent for a letter sent from the Consumer Technology Association to Chairman Cummings about this issue.

Chairman CUMMINGS. Without objection, so ordered.

Chairman CUMMINGS. Mr. Massie?

Mr. MASSIE. Thank you, Mr. Chairman.

Dr. Romine, you reported on the accuracy of the algorithms that NIST tested. You said they are 99 to 99.7 percent accurate. First of all, that accuracy rating, I can imagine two ways the algorithm fails. One would be a false positive, and one would be failing to recognize an actual match. Which number are you reporting?

Mr. ROMINE. So, for the—let me double check because I want to be sure I get this right. The accuracy at 99.7 I believe is false-negative rates, but I am going to have to double check and get back to you on that.

Mr. MASSIE. Okay, that would be great. You can get back to me later.

Did you test certain conditions like siblings, the accuracy for siblings?

Mr. ROMINE. We do have—perhaps the most relevant data that I can give you is we do know that there is an impact on twins in the data base or in the testing, whether they are identical twins or even fraternal twins——

Mr. MASSIE. Well, let me give you the data point I have. I have two sons. One is two-and-a-half years younger than the other. He can open his brother's phone. They don't look that much alike. They look like brothers. He furrows his eyebrows and changes the shape of his mouth to the way he thinks his brother looks, and he opens his phone every single time. So that accuracy is not 99 percent. That is zero percent.

Now, that may be an older algorithm. I am sure they have improved in a couple of years since this happened.

I want to submit for the record an article in Forbes by Thomas Brewster called "We Broke Into a Bunch of Android Phones with a 3-D Printed Head."

Chairman CUMMINGS. Without objection, so ordered.

Mr. MASSIE. Thank you, Mr. Chairman.

So I think these aren't as accurate—for certain special conditions, like somebody wearing a mask or make-up or maybe a sibling, the accuracy does not approach or may not approach 99 percent with some of these algorithms. What do you think?

Mr. ROMINE. The situations you are describing are situations where there is intent to deceive either through lack of——

Mr. MASSIE. Do you think there is intent to deceive in the world?

Mr. ROMINE. I certainly do.

Mr. MASSIE. Yes. That is what we are worried about at TSA is intent to deceive, not the honest actor.

But let me go to something else here, and this question is for Ms. Del Greco. The Supreme Court case, Brady v. Maryland, held that due process rights require government to promptly disclose potential exculpatory evidence with the defense. So in the case where multiple photos are returned, or there may be nine possible matches, does the defense get access or knowledge that there were other possible matches?

Let me give you an example. In a prior hearing, I had somebody testify to us that a sheriff's office gave an example where a person, a person with 70 percent confidence was the person they ended up charging, even though the algorithm thought somebody else was at 90 percent confidence. So they charged the person that the algorithm said was 70 percent likely and passed over the one that was 90 percent likely in this case.

Can you guarantee us that the FBI would provide that type of information to the defense?

Ms. DEL GRECO. First, the FBI doesn't make a match. We provide an investigative lead to our law enforcement partners. But with all evidence obtained during an investigation——

Mr. MASSIE. Do you ever provide more than one lead?

Ms. DEL GRECO. We provide more than one lead sometimes. Yes, sir.

Mr. MASSIE. Okay.

Ms. DEL GRECO. Two or more. It depends on the state. Some states want 20 candidates, some want two back. It depends on their state system.

Mr. MASSIE. So does the defense get access to the knowledge that there were other leads, and do you assign a probability or a confidence level with that facial recognition?

Ms. DEL GRECO. I think the prosecution team must determine on a case-by-case basis.

Mr. MASSIE. So you are not sure if they always get that.

Ms. DEL GRECO. No, I am not. We don't provide a true match, an identification back. It is up to the law enforcement entity to make that decision.

Mr. MASSIE. A quick question. How many photos does the face data base have access to, including the state driver's license data bases?

Ms. DEL GRECO. That changes daily. I don't have that, sir.

Mr. MASSIE. Is it in the millions, tens of millions?

Ms. DEL GRECO. I don't know, sir. I can provide that to you.

Mr. MASSIE. Do you have access to Kentucky's data base?

Ms. DEL GRECO. I can check for you, sir.

We do not.

Yes, we do, sir.

Mr. MASSIE. Okay. So you have access to all the photographs in the driver's license data base in Kentucky. Which elected official agreed to that?

Ms. DEL GRECO. I believe we worked with the state authorities in Kentucky to establish the MOU.

Mr. MASSIE. But not an elected official.

Ms. DEL GRECO. The state authority is public, and it is pre-determined and established prior to face recognition.

Mr. MASSIE. So you say the laws that you are relying on were passed before facial recognition became——

Ms. DEL GRECO. They were. They were, sir.

Mr. MASSIE. Okay. That is, I think, a problem.

All right. I yield back, Mr. Chairman.

Chairman CUMMINGS. Thank you very much.

Mr. Rouda?

Mr. ROUDA. Thank you, Mr. Chairman.

Dr. Goodwin, in May 2016, the GAO made six recommendations to the FBI, three related to privacy, of which I believe one was implemented, and three related to accuracy. Can you talk about briefly the five that are not yet implemented?

Ms. GOODWIN. Yes, sir. So, the three related to privacy focused on developing the PIA process so that it is more aligned with the requirements. The other one focuses on publishing the SORN in a timely manner. So basically developing the process for the PIA, developing a process for the SORN, and making certain that those are published in a timely fashion.

And then the other three are accuracy related, and they are about testing or expanding the candidate list size because, as you know, the list size, we took issue with the fact that they didn't test the smaller list size. So that is one of them.

The other one is regularly assessing whether the NGI-IPS actually meets their needs, so that is an accuracy concern.

And the other one focuses on the face data base, making certain that those are also meeting the needs.

So those three questions related to accuracy I think kind of speak to this conversation here. The information that the FBI is using, that information needs to be accurate, especially if they are using it for their criminal investigations. It is really important that the information be accurate that they are using.

Mr. ROUDA. And these recommendations were made three years ago. Is the lack of implementation—why has that been the case for three years?

Ms. GOODWIN. That probably is a question better left to the FBI.

Mr. ROUDA. I will come around to that.

Dr. Romine, you stated 99.7 percent accuracy, but that is specific algorithms. When you look at the breadth of algorithms that are used, I then assume based on your statement that there are accuracy rates much lower than that. Again, on the algorithm, can you elaborate on that?

Mr. ROMINE. Yes, sir. The range of performance in terms of accuracy for the algorithms is pretty broad. Some of the participants have made substantial progress and have remarkably accurate algorithms in terms of the 99 and above percent for false-negative rates. Others are as much as—I believe it is about 60fold less accurate than that. But those are from a variety of sources, including one university algorithm for research participation.

Mr. ROUDA. And is their data—and I am going to ask you this, as well as Ms. Del Greco. Is their data showing facial recognition accuracy versus traditional photographs and enhanced photography?

Mr. ROMINE. I am not quite sure I understand your question, sir.

Mr. ROUDA. Well, whether it is an old-fashioned technology of just using photographs versus facial recognition——

Mr. ROMINE. Oh, I see.

Mr. ROUDA [continuing]. is there any data that we have available that shows facial recognition is a large step in the right direction, even with the challenges we are having here?

Mr. ROMINE. We do have—NIST also tests human performance in facial recognition through comparison photographs. Interestingly, what we find, and I refer to my testimony, is that if you combine two humans, you don't really do much better than anyone individually. If you combine two algorithms, you don't really do much better than either individually. If you combine a human and a facial recognition algorithm, you do substantially better than either.

Mr. ROUDA. Okay. And, Ms. Del Greco, going to you, you can answer the same question, but also I would like to pivot back as to why the FBI has not implemented the five other recommendations of the GAO.

Ms. Del Greco. The two recommendations regarding the PIA and the SORN, DOJ disagrees with GAO's legal assessment of the publication of the PIA and the SORN. We had privacy attorneys embedded in our process the whole time. We published a PIA and a SORN, and we continue to update those accordingly, and we have provided updates to GAO.

With regard to the candidate list size, since the last hearing in 2017 the FBI conducted a test of our current accuracy in the system at all list sizes, and we were able to validate that the percentage was higher than what we published in 2017.

Mr. ROUDA. Okay. I just want to get one more quick question in. If a bad actor with bad intentions and the skill set to use disguises, doesn't that circumvent this entire process?

Ms. DEL GRECO. We provide a candidate back, and we use trained FBI examiners. As Dr. Romine alluded, the system combined with the trained FBI examiner provides a better response back to the law enforcement entity.

Mr. ROUDA. Okay. Thank you.

I yield back, Mr. Chairman.

Chairman CUMMINGS. Thank you very much.

Mr. Amash?

Mr. AMASH. Thank you, Mr. Chairman.

Ms. Del Greco, does the FBI use real-time face recognition on live video feeds, or have any plans to do so in the future?

Ms. DEL GRECO. No, we do not.

Mr. AMASH. Has the FBI ever experimented with real-time face recognition?

Ms. DEL GRECO. Not to my knowledge, sir.

Mr. AMASH. Do any of the FBI's domestic law enforcement partners utilize or plan to utilize real-time face recognition technology?

Ms. DEL GRECO. Not for criminal justice purposes.

Mr. AMASH. Does the Department of Justice believe the FBI has statutory authority to do real-time face recognition itself?

Ms. DEL GRECO. Not to my knowledge.

Mr. AMASH. Does the Department of Justice believe the FBI has statutory authority to give states grants that would support real-time face recognition?

Ms. DEL GRECO. No, sir.

Mr. AMASH. Ms. Del Greco and Mr. Gould, please name the companies who lobby or communicate with your agencies about face recognition products they would like to provide.

Ms. DEL GRECO. We have the testing that we have done through NIST, but those are the only agencies that we are familiar with, and we would defer to the NIST vendors that participated in the Facial Recognition Vendor Test in 2018.

Mr. GOULD. Sir, the system the TSA is prototyping in conjunction with CBP uses an NEC camera and a matching algorithm that was also developed by NEC.

Mr. AMASH. So NEC would be the only company?

Mr. GOULD. That is the company we are working with right now. Yes, sir.

Mr. AMASH. Okay. Mr. Gould, how many air passengers have participated in TSA's face recognition pilots?

Mr. GOULD. Sir, I would have to get back to you with a number on that, for the record.

Mr. AMASH. And you couldn't tell us how many participants are U.S. citizens?

Mr. GOULD. No, sir.

Mr. AMASH. Under what statutory authority does TSA use face recognition technology on American citizens?

Mr. GOULD. We use the authority of the Aviation Transportation Security Act, which requires us to positively identify passengers who are boarding aircraft and proceeding through the checkpoint.

Mr. AMASH. And can you tell me what statutory authority TSA uses for face recognition technology on domestic travelers generally?

Mr. GOULD. Sir, I would say it was the same authority, the Aviation Transportation Security Act.

Mr. AMASH. And does TSA have any plans for real-time face recognition technology in airports?

Mr. GOULD. Sir, if you mean real-time as facial capture and matching at the checkpoint, then yes, that is what we are pursuing.

Mr. AMASH. And has TSA considered the privacy implications of real-time face recognition technology?

Mr. GOULD. Yes, sir, absolutely. We have done privacy impact assessments associated with this. There is signage at the airports that clearly identifies that we are using facial recognition technology in a pilot manner to identify passengers, and we don't store any photographs on the camera.

Mr. AMASH. And will travelers be able to opt out?

Mr. GOULD. Yes, sir. Travelers will always have the opportunity to not participate in the program.

Mr. AMASH. And you think that is true now and into the foreseeable future?

Mr. GOULD. Yes, sir.

Mr. AMASH. Do you have plans to implement face recognition technology at additional points in airports besides gates or security checkpoints?

Mr. GOULD. We are prototyping facial recognition technology at bag drops. So when you drop a bag off to be placed on an aircraft, we can use facial technology—we are exploring the use of facial technology there. And then for TSA purposes, the only other location is the checkpoint.

Mr. AMASH. Okay. Thanks.

I yield——

Mr. MEADOWS. Will the gentleman yield?

Mr. AMASH. Yes, I yield to Mr. Meadows.

Mr. MEADOWS. So, Mr. Gould, let me come back. If you are doing it at bag drops, that is not a one-on-one comparison? I mean, what are you comparing it to? If you are looking at checking facial recognition at bag drops, there wouldn't be necessarily the identification that you were talking about earlier. What pilot program are you working with with that?

Mr. GOULD. The pilot program in place right now is with Delta Airlines and CBP and TSA at Atlanta's Terminal F, and it is a matching of the passenger's bag against their identification or their photograph in the CBP TVS system.

Mr. MEADOWS. Well, that contradicts your earlier testimony, Mr. Gould, because what you said that you were doing is just checking the biometrics within the identification against a facial recognition, but it sounds like you are doing a lot more than that.

Mr. GOULD. Sir, this is for international travelers.

Mr. MEADOWS. No, I understand. I just came back—I came through JFK. I didn't see any of the signs that you are talking about, all right? So I guess what I am saying is what statutory authority gives you the ability to do that? You keep referring to 2001. I actually am on the Transportation Committee, and I can tell you we never envisioned any of this. I am looking at the very statute myself here. How can you look and suggest that the statute gives you the ability to invade the privacy of American citizens?

Chairman CUMMINGS. The gentleman's time has expired, but you may answer the question.

Mr. GOULD. I am sorry, sir?

Chairman CUMMINGS. You may answer the question.

Mr. GOULD. Okay, thank you.

Sir, with respect to the pilot in Atlanta, it is international travelers, and the purpose of that pilot is to positively match, using biometrics, the passenger to that bag at the bag drop. The traveler's photograph is captured, image is captured. It is transmitted to the CBP TVS system for matching, and it returns a match result. That is it, no privacy information or any other data associated with it.

With respect to JFK, there is no pilot going on there right now. It is solely in Atlanta in Terminal F.

Chairman CUMMINGS. Ms. Hill?

Ms. HILL. Thank you, Mr. Chairman.

I want to follow up, actually, on several of these questions.

Mr. Gould, does the TSA say how many American citizens' faces it captured during the pilot? And if so, do you know the numbers?

Mr. GOULD. No, ma'am, I don't know the numbers. I would have to submit that for the record.

Ms. HILL. Yes, please. Also, TSA uses the facial recognition systems of Customs and Border Protection, CBP, which may not restrict how private corporations use passenger data. According to an August 2018 article from the New York Times, CBP "has said it cannot control how the companies use the data because they are not collecting photographs on CBP's behalf." An official stated that "he believed that commercial carriers had no interest in keeping or retaining the biometric data they collect, and that the airlines have said they are not doing so. But if they did, he said, that would really be up to them. TSA itself has said that it intends to pursue innovative models of public-private partnerships to drive collaboration and co-investment."

Mr. Gould, if TSA uses CBP systems to scan the faces of American citizens, how can it ensure that the private data of these passengers is not stored or sold by private airlines?

Mr. GOULD. Ma'am, I would have to refer to CBP for any assessment of the security and the privacy of that system.

With respect to the public-private partnership, when we refer to that we are talking about partnering with industry, airlines and airports solely on the front-end capture system, so basically the cameras that are being utilized.

Ms. HILL. But you talk about co-investment.

Mr. GOULD. So, in accordance with TSA's authorities, we are allowed to enter into agreements with airports and/or airlines to procure equipment on our behalf, and that equipment would be the camera system only, solely for the capture. The matching and the data base, that is a government system, and right now we are using the CBP TVS system.

Ms. HILL. So have you thought about how you would ensure that the private data is not stored or sold by airlines?

Mr. GOULD. Absolutely, ma'am. First of all, when your photo is captured at a checkpoint in the pilots, it is encrypted and sent off for matching, and the data base that CBP uses, the TVS system, that is cyber-secure in accordance with applicable standards, and we do not transfer any personally identifiable information between us and the airlines.

Ms. HILL. Dr. Goodwin, what regulations do you believe should be put in place in order to prevent the abuse of passenger data by airlines and other private companies?

Ms. GOODWIN. So, as you know, GAO, we wouldn't provide an answer to that question. The way we think about it is we have issued recommendations related to privacy and accuracy, and if those recommendations are implemented, that would actually go a long way to meeting some of the needs of the public, as well as the needs of this committee.

Ms. HILL. Sorry. Can you clarify?

Ms. GOODWIN. So we have those six recommendations related to privacy and accuracy. Only one has been implemented. So we believe that if the remaining five are implemented, that would actually go a long way to answering the questions and addressing some of the concerns around privacy for the citizens and accuracy for the data that are being collected.

Ms. HILL. And, Mr. Gould, do you have issues with those recommendations? Is there something that is preventing TSA from incorporating those?

Mr. GOULD. So, as I stated before, in accordance with Section 1919 of the TSA Modernization Act, we have executed in conjunction with CBP a thorough review of the privacy impacts associated with biometrics collection or biometrics identification at the airport, as well as any error rates and security concerns associated with that, and that report will be coming from DHS in the near future.

Ms. HILL. Great.

The Washington Post further stated that around 25,000 passengers traveled through Atlanta's airport pilot program terminal each week. According to the article, "only about two percent of travelers opt out." Even assuming that the systems used by TSA are 99 percent accurate, which they are likely not, the high volume of passenger traffic would still mean that at least hundreds of passengers are inaccurately identified each week.

Does TSA keep metrics on the number of American citizens that are inaccurately identified?

Mr. GOULD. In accordance with our analysis, the pilots were capturing match rates and non-match rates. With respect to the actual numbers of Americans that do not return a positive match rate, I would have to submit something for the record.

Ms. HILL. Please do.

And, Dr. Romine, what would be the most effective way for TSA to measure how accurate its facial recognition systems are when testing the identity of American citizens?

Mr. ROMINE. We are not expert in testing full systems. We test algorithms. We evaluate those algorithms for accuracy of matching. The entire system is something that is a little bit outside my purview.

Ms. HILL. Okay. I personally understand the value of this technology, but I think we really need to have some clear regulations and guidance that are essential to prevent the abuse of data collected and to protect our privacy. While I appreciate the GAO's recommendations, I think we are going to need some more teeth to ensure that those are implemented.

Thank you. I yield back.

Chairman CUMMINGS. Mr. Hice?

Mr. HICE. I will let Mr. Roy go first.

Chairman CUMMINGS. Mr. Roy?

Mr. ROY. Thank you, Mr. Chairman. I appreciate it.

Thank you to my colleague from Georgia for letting me go now.

I appreciate all you all taking the time to testify today. I appreciate your service to our Nation. As a former Federal prosecutor, I appreciate the commitment to law enforcement and what you are trying to do to keep the United States and its citizens safe. I do think that there have been some very important issues involving privacy raised here today on both sides of the aisle, and I appreciate you all addressing those concerns.

One of the lines of questions was my colleague from Michigan, Congressman Amash, asking a little bit about real-time use of this technology, and I wanted to explore that just a little bit further and maybe even ask a simple, maybe a not all that informed question.

Is the U.S. Government in any way, based on the knowledge of anybody at the table, using facial recognition technology on American citizens without their knowledge today? And if so, where and how?

Ms. Del Greco?

Ms. DEL GRECO. The FBI systems are not designed for real-time capture of the American people.

Mr. ROY. So to your knowledge, the U.S. Government, from your base of knowledge, is not using facial recognition technology to capture information on American citizens, using it and processing it without their knowledge?

Ms. DEL GRECO. The FBI does not. I can speak on behalf of the FBI. We require it for criminal purposes only, in accordance with a law enforcement purpose.

Mr. ROY. Mr. Gould?

Mr. GOULD. Sir, with respect to TSA, we are doing it solely with the passengers' consent. The cameras are visible, and the passenger needs to actually assume a position in front of the camera for accurate facial capture.

Mr. ROY. Any other witnesses? Dr. Goodwin, are you aware of anything?

Ms. GOODWIN. We are not. In the work that we have done, that has been beyond the scope.

Mr. ROY. Okay.

Sir?

Mr. ROMINE. It is also outside of NIST's scope.

Mr. ROY. Do you all know of any plans to use that technology without consent of an American citizen?

Mr. GOULD. Not with respect to TSA, sir.

Mr. ROY. FBI?

Ms. DEL GRECO. The FBI will not develop technology for CJIS Division outside of a criminal purpose, sir.

Mr. ROY. Ms. Del Greco, let me ask you a quick question. You said in response to Mr. Amash in one of his questions about real-time use, you said "not for criminal justice purposes." Can you expand on that caveat?

Ms. DEL GRECO. That we only collect a photo in conjunction with criminal justice. Our law enforcement partners, the state and local and Federal entities, must be authorized to have access to our sys-

tem, and they must have a criminal justice purpose in order to search our system, the NGI Interstate Photo System.

Mr. ROY. I would like to yield to my colleague from Louisiana.

Mr. HIGGINS. I thank my colleague for yielding a bit of his time.

Ms. Del Greco, according to FBI records, in 2017 10,554,985 criminal arrests were made, and you ran about a 59 percent conviction rate. I think that this body and the American people must be reminded that every American that has been arrested is arrested by probable cause. The standards of probable cause are much less than that of conviction. Is that true?

Ms. DEL GRECO. That is correct, sir.

Mr. HIGGINS. Would the totality of circumstances and corroborative evidence be used in the course of a criminal investigation, and any technology, including facial recognition technology, would that be added as a tool in the toolbox to add perhaps a strength or a weakness to that case file?

Ms. DEL GRECO. State and local entities have the option to submit a probe photo in accordance with a criminal investigation.

Mr. HIGGINS. Okay. Moving quickly, one of my colleagues mentioned that there was a 70 percent match on a subject and that is the subject that was arrested, versus a 90 percent match that was not arrested. Does not arrested mean not investigated?

Ms. DEL GRECO. I am not aware of that, sir. We provide candidates back——

Mr. HIGGINS. During the course of a regular criminal investigation, is reasonable suspicion grounds for investigation of any citizen?

Ms. DEL GRECO. I am not a law enforcement officer, sir.

Mr. HIGGINS. All right. I am, and it is.

Probable cause is the standard for arrest. Beyond a reasonable doubt or the shadow of a doubt is the standard for conviction.

I very much appreciate everyone's testimony today.

This is an emerging technology. Mr. Chairman, Mr. Ranking Member, we should watch this technology closely and protect the rights of American citizens. We should also recognize that this can be a very valuable tool for law enforcement and to fight crime in our country, and I yield.

Chairman CUMMINGS. Ms. Norton?

Ms. NORTON. Thank you, Mr. Chairman.

Look, we are not Luddites here. We recognize, I think, advancements that science is making. Perhaps this particular facial recognition advancement, such as it is, is not ready for prime time, and that is what we are trying to ascertain here, and yet it is being used as if it were.

The FBI, Dr. Goodwin, uses this facial recognition system but cannot tell us, we have learned today, much about its accuracy. And the GAO—and we rely heavily on the GAO, of course—has said DOJ officials stated there is value in searching all available external data bases regardless of the level of accuracy. That is where my question goes, regardless of the level of accuracy.

The FBI has said, Ms. Del Greco, that the facial recognition tool is used for investigative leads only. Now, what is the value of searching inaccurate data bases? I can see the downside: mistaken identity, misidentification. Why is there any value in searching

whatever data base is available to you based on investigative leads only?

Ms. DEL GRECO. The FBI uses our trained face examiners to look at candidates that come back on a search for an FBI open investigation, and it evaluates all of the candidates, and it provides the search back.

Ms. NORTON. Can an investigative lead lead to conviction?

Ms. DEL GRECO. The FBI field office and the FBI agent is the one that is primary to that case. They know all the details about the case. We would not be making that decision. It would be up to them to use that as a tool.

Ms. NORTON. So it could, as far as you know, lead to a conviction, or maybe not.

Ms. DEL GRECO. That is correct, ma'am. I agree.

Ms. NORTON. So not only could it lead to a conviction, it could lead to inaccurate convictions.

Ms. DEL GRECO. We hope not, ma'am. We hope not.

Ms. NORTON. Yes, it could lead to a conviction, but perhaps it would be inaccurate since we are using the data base for investigative purposes as well.

Now, here is what bothers me most. There has been a prominent study done which included an FBI expert, by the way, Ms. Del Greco. It found that leading facial recognition algorithms, like ones sold by Amazon and Microsoft and IBM, were more inaccurate when used on darker-skinned individuals, women, and people aged 18 to 30, when compared with white men. So we do have some indication when we look at what our population is.

Dr. Romine, do you agree with the findings of this study?

Mr. ROMINE. There are demographic effects. This is very time-dependent. It depends on the time at which this was done and the algorithms that were evaluated. NIST is prepared to release demographic information or——

Ms. NORTON. My concern is that there is excessive, some would say over-policing in minority communities. I understand why. But it has resulted in African Americans being incarcerated at four times the rate of white Americans. African Americans are over-represented in mug shots that some facial recognition systems scan for potential matches.

Ms. Del Greco, do you agree that both the presence, the over-representation of African Americans in mug shot photos, the lower accuracy rates that facial recognition systems have when assessing darker-skinned people such as African Americans, that it is possible that false convictions could result from the FBI's use of these external systems if they are not audited?

Chairman CUMMINGS. The gentle lady's time has expired. You may answer the question.

Ms. DEL GRECO. The FBI retains photos in our repository, mug shot photos, but they are associated with a criminal arrest and a ten print fingerprint. We do provide a candidate——

Ms. NORTON. Are they audited?

Ms. DEL GRECO. Yes, they are, ma'am. We have a robust audit process with the state, Federal, local, and tribal agencies. We send auditors out to those agencies and we look at security requirements in accordance with the FBI CJIS security. We look at the policies,

the procedures, and the standards to ensure that they have the required training and they are following our process.

Chairman CUMMINGS. Mr. Hice?

Mr. HICE. Thank you, Mr. Chairman.

I think we all are very much aware of the effects of surveillance on people. Their behavior certainly changes. Non-criminal speech, non-criminal behavior, it alters the way people behave when there is surveillance. Just even as a pastor for many years, I know with the prying eyes of the IRS and how that has had a chilling effect on speech, even within non-profit organizations and churches. So this is an extremely serious thing when we know the possibility of surveillance is out there.

Ms. Del Greco, has the FBI ever—you mentioned a while ago the FACE Services Unit or something to that effect. Does that particular unit or any other unit in the FBI farm for images, photographs, other I.D.-type information on American citizens through social media or whatever other platform?

Ms. DEL GRECO. No, we do not, sir.

Mr. HICE. Does the FBI, have they ever purchased from a third-party contract or wherever else images, photographs, I.D. information?

Ms. DEL GRECO. No, sir. The FBI retains only criminal mug shot photos.

Mr. HICE. Okay.

Mr. Chairman, I would like to ask to be submitted to the record an article by Joseph Cox of Vice News, "SocioSpyder: The Tool Bought by the FBI to Monitor Social Media."

Chairman CUMMINGS. Without objection, so ordered.

Mr. HICE. I would also like to submit for the record an archived copy of the sociospyder.com Web domain that states that this software is used for automated collection of social media user data. I would like that to be submitted.

Chairman CUMMINGS. Without objection, so ordered.

Mr. HICE. Thank you, Mr. Chairman.

And finally also, I would like to submit to the record the purchase of order logs of the FBI, SocioSpyder software and service agreement and individual user license, purchased by Allied Associates International.

Chairman CUMMINGS. Without objection, so ordered.

Mr. HICE. Thank you.

Ms. Del Greco, there has been software purchased by the FBI, and I don't know where you are coming from to not be aware of that.

Ms. DEL GRECO. Sir, I would have to find out from the other entities within the FBI. I represent the technology that is used for criminal justice purposes at the CJIS Division.

Mr. HICE. So there is a whole other avenue of facial recognition technology taking place within the FBI that you know nothing about.

Ms. DEL GRECO. Not that I am aware of, sir.

Mr. HICE. Well, evidently, if you don't know anything about this, there is.

Ms. DEL GRECO. We can look into it, sir.

Mr. HICE. Okay, we most certainly can. So are you saying, then, that to your knowledge there is no software—although there is—that is being used by the FBI to collect information on U.S. citizens?

Ms. DEL GRECO. I am only aware of the use of our system for criminal justice purposes, sir.

Mr. HICE. Okay, and your system would include the systems of the driver's license data base of multiple states?

Ms. DEL GRECO. Our system does not retain driver's license photos.

Mr. HICE. But you have access to it. So there are two different systems. You have your internal system, and then you have this system that you can access.

Ms. DEL GRECO. We do not have direct access. We——

Mr. HICE. A 2016 study by Georgetown's Law Center on Privacy and Technology found that you do have access to that, a total of 117 million Americans, which comes to about one out of every two adults that you have access to that information.

Ms. DEL GRECO. That is incorrect, sir. We disagree with that. The FBI, through an active FBI investigation, can submit a probe photo to our——

Mr. HICE. So how many do you have access to?

Ms. DEL GRECO. We can submit a probe photo to the state DMVs, and they provide a candidate back. We do not have access to those photos.

Mr. HICE. Well, the study disagrees with you. There is really a pre-crime data base, if you will.

I have a little bit of time. I do want to yield to the Ranking Member with the remaining time. Thank you.

Mr. JORDAN. I thank the gentleman.

Ms. Del Greco, just to go to this real-time surveillance, so has the FBI or any other Federal agency, to your knowledge, ever used real-time surveillance, sort of a continuous look at a group of people at some location? Has that ever been done?

Ms. DEL GRECO. No, sir, not to my knowledge.

Mr. JORDAN. And to your knowledge, no other Federal agency has done that, the IRS, any other agency has not done that either? Do you know?

Ms. DEL GRECO. I cannot speak on behalf of the other agencies, sir.

Mr. JORDAN. And let me just, real quick if I could, Mr. Chairman, the numbers, Dr. Goodwin. What number of photos does the FBI have access to in just their data base?

Ms. GOODWIN. In just their data base, a little over 20-plus, 36 million.

Mr. JORDAN. Thirty-six million. And then in the data bases that they can then send information to and that are screened and used and there is interface and interaction with at the state level, what is the total number of photos in all those data bases?

Ms. GOODWIN. So access to photos across all the repositories, about 640 million.

Mr. JORDAN. Six-hundred and forty million photos. There are only 330 million people in the country. Wow. The FBI has access to 640 million photos, and this is the FBI that didn't comply with

the five things they were supposed to comply with when they set up the system, and they are still not in compliance with.

Ms. GOODWIN. So if you think about the face services system, and then all of the searchable repositories, that is over 640 million photos, and the FBI really only searches for criminal. They are looking for the criminal photos. They are looking through all of this for their criminal investigations. But across all the repositories, we are talking over 600 million.

Mr. JORDAN. Thank you, that is very helpful. I appreciate that.

Chairman CUMMINGS. We are talking about people who have been arrested, right? Not necessarily convicted. Is that right, Ms. Del Greco?

Ms. DEL GRECO. Arrested, by searching these data bases, sir?

Chairman CUMMINGS. Yes, ma'am.

Ms. DEL GRECO. We would have to go back and do a survey. We do every 90 days go out to our state and local agencies to see if there is any input they can provide to us. We do know there are arrests made, but it is not on the identification of the photo. It is a tool to be part of the case that they have.

Ms. GOODWIN. If I could add one more thing about the 640 million, most of those are civil photos, but those are available——

Mr. JORDAN. That is what scares me.

Chairman CUMMINGS. Most of them—say that again?

Ms. GOODWIN. Those are primarily civil photos. So we are talking about passports and driver's licenses.

Mr. JORDAN. Yes, sure.

Chairman CUMMINGS. Just regular, everyday people. Wow.

Ms. Kelly?

Ms. KELLY. Thank you, Mr. Chairman, for holding this second hearing on facial recognition.

With the government's use of facial recognition increasing, it is important that this nascent technology is not rushed to market and that all communities are treated equally and fairly.

Mr. Romine, in your testimony you mentioned the report that is due for publication this fall is on demographic effects and mug shots. Can you talk a little bit about this report and your objectives?

Mr. ROMINE. The objective is to ensure complete transparency with regard to the performance of the algorithms that we evaluate and to see if we can use rigorous statistical analysis to demonstrate the presence or absence of demographic effects. That statistical analysis has not been completed yet. We have preliminary data that have suggested that demographic effects such as difference in age across ages, difference in sex, and difference in race can affect or can have differences in terms of the performance of the algorithms. However, the increased performance across the board for the best-performing algorithms is, we expect, diminishing that effect overall. In the fall we will have the final report of demographic effects.

Ms. KELLY. I commend you for looking into this. When you are doing evaluations for companies, are you testing for demographic consistency?

Mr. ROMINE. We do—we don't test for specific companies on their behalf. We test or evaluate the algorithms that are submitted to us

through this voluntary program. So we don't test specifically for algorithms' demographic effects. We are talking about the demographic effects across all of the algorithms that are submitted.

Ms. KELLY. And then what are you doing to make sure that no categories of people are suffering from lower rates of accuracy?

Mr. ROMINE. The best we can do in that is to ensure transparency and public access to data about the level of the demographic effects. We have no regulatory authority to do anything about that other than to just make the data available for policymakers to make appropriate decisions.

Ms. KELLY. Did you have a comment about that? Okay.

Mr. Gould, TSA has been partnering with CBP on biometrics for international travelers. How much training did operators receive prior to beginning the pilot program at JFK and LAX?

Mr. GOULD. The training was significant. I would say multiple days of training in how the system works, how to analyze the match results, and how to effectively use the system.

Ms. KELLY. What were the top complaints that were received during this pilot program?

Mr. GOULD. The complaints from the public, ma'am?

Ms. KELLY. The top complaints, yes.

Mr. GOULD. Ma'am, I am really honestly not aware of any specific category of complaints that rose to the surface. In general, the public seems to enjoy the enhanced passenger experience by using biometrics.

Ms. KELLY. Any complaints by employees?

Mr. GOULD. I would say employees in general, when you introduce new technology, the change can be somewhat challenging to use, but having just been down to Atlanta and talked to many of the operators down there, as well as the Federal security director in charge of the airport, they embrace the technology and find it to be a significant enhancement to security at the checkpoint.

Ms. KELLY. Okay. The report on disparities is due on July 2d, 2019. Are you on schedule for publication, and are there any previews that you can share?

Mr. GOULD. I don't have any previews available that I can share. The report has been completed in accordance with Section 1919 of the TSA Modernization Act. The report has been compiled and it is on its way through the Department to Congress. Yes, ma'am.

Ms. KELLY. Thank you very much, and I yield back.

Mr. GOULD. Thank you.

Chairman CUMMINGS. Thank you very much.

Mr. Meadows?

Mr. MEADOWS. Thank you, Mr. Chairman.

Ms. Del Greco, I am not going to beat up on you, but I am going to come back and give you two pieces of advice. One is—and it is the same advice I give to every witness who sits in that seat right next to GAO. If GAO isn't happy, I am not happy. So here is what I would recommend on the five outstanding things, that you work with GAO to close those out, the five recommendations that they have. Are you willing to do that?

Ms. DEL GRECO. Absolutely, sir.

Mr. MEADOWS. All right. The fact that you only closed one of them out last week prior to this hearing is what I understand—is

that not accurate? I could tell you were smiling, so you didn't agree with that statement.

Ms. DEL GRECO. Not that I disagree. We have been completing audits. We completed 14 of the 21, and I think GAO felt that that was enough to satisfy the issue.

Mr. MEADOWS. All right. Well, Dr. Goodwin, if you will report back to this committee, what I would like in the next 60 days is the progress we are making.

Ms. Del Greco, that is as gracious as I can be when it comes to that. Listen, we want you to have all the tools to accurately do what you need to do.

The second thing that I would mention is you mentioned about not having any real-time systems, and yet we had testimony just a couple of weeks ago from Georgetown that indicated the Chicago Police Department, the Detroit Police Department has real time. They purchased it where they are actually taking real-time images. Do they ping the FBI to validate what they picked up in real time with what you have in your data base?

Ms. DEL GRECO. I mean, there are authorized law enforcement entities that have access to our system. We train them. We expect them to follow our policies. We audit them.

Mr. MEADOWS. I get that. But what I am saying is that we are concerned about real time, and you have police departments in Chicago and Detroit that are doing real-time surveillance and then getting you to authenticate that through your data base; is that correct?

Ms. DEL GRECO. They submit a probe photo in accordance with a criminal——

Mr. MEADOWS. From real-time surveillance.

Ms. DEL GRECO. Not to my knowledge. I am not aware of that.

Mr. MEADOWS. Well, that is opposite of the testimony. So what I want you to do—and did they purchase that real-time surveillance technology with Federal funds? If you will get back to the committee on that, can you do that?

Ms. DEL GRECO. Yes, sir.

Mr. MEADOWS. All right. Thank you.

Mr. Gould, I am going to come to you, because some of your testimony—actually, I have been to Dulles where we looked at CBP, actually looking at real-time facial recognition when travelers come in and out. So I guess you are saying that right now you are not doing that at Dulles anymore; is that correct? Because you mentioned only Atlanta and——

Mr. GOULD. Sir, I can't comment on the CBP program, because they do it for entering and exit purposes for international travel. TSA is not doing it there.

Mr. MEADOWS. Okay, so here is what I would recommend. Out of all the priorities that TSA has, and all the inefficiencies that actually this committee and other committees have, facial recognition certainly cannot be the top priority in terms of what we are looking at to make sure our traveling public is safer. Would you say that that is the top priority that you have in terms of your Achilles heel?

Mr. GOULD. Sir, positive identification of travelers——

Mr. MEADOWS. That is not the question I asked. Is that the top priority? Yes or no?

Mr. GOULD. That is one of multiple significant priorities for TSA.

Mr. MEADOWS. So what is your top priority?

Mr. GOULD. I would say——

Mr. MEADOWS. There can only be one top, Mr. Gould. This is a softball question.

Mr. GOULD. I would say at this point enhanced property screening at the checkpoint, CT machines for the checkpoint to do a better assessment of carry-on baggage.

Mr. MEADOWS. All right. So you mentioned the fact that you potentially have actually taken photos of American citizens dropping off their bags; is that correct? In my questioning earlier you talked about the fact that you might have—part of TSA is looking at the screening process where it is not just a one-on-one, where you are actually taking photos of people at bag drops; is that correct?

Mr. GOULD. Only if they choose to participate, and only in one location, and that is Terminal F in Atlanta.

Mr. MEADOWS. All right. So you can guarantee, because I have flown out of Terminal—well, Concourse F, I think is what it is. But I have flown out of that on Delta. So you can guarantee that I was not photographed? Because I have never given anybody my permission on international travel, to my knowledge. So can you guarantee that I am not picked up in that?

Mr. GOULD. Unless you were photographed while you were dropping off the bag at Delta——

Mr. MEADOWS. But that is my question.

Mr. GOULD. No, sir.

Mr. MEADOWS. My question is I gave no one permission to take my picture while I am dropping off my bag. I am an American citizen.

Mr. GOULD. Yes, sir.

Mr. MEADOWS. What rights, what legal rights do you have to take that photo?

Mr. GOULD. You should not have been photographed.

Mr. MEADOWS. Okay. And so you can't guarantee that I wasn't.

So here is what I would recommend, Mr. Gould, is this. I am all about making sure that we have screening, but I can promise you I have gone through screening more than most Americans, and there are inefficiencies in TSA that have nothing to do with facial recognition. And until you get that right, I would suggest that you put this pilot program on hold, because I don't know of any appropriations that specifically allowed you to have this pilot program. Are you aware of any? Because you keep referring back to a 2001 law, and I am not aware of any appropriations that have given you the right to do this pilot program.

Mr. GOULD. I am not aware of any specific appropriation that——

Mr. MEADOWS. Exactly. I would recommend that you stop it until you find out your statutory authority.

I yield back.

Chairman CUMMINGS. Thank you very much.

Before we go to Ms. Lawrence, let me follow up on the gentleman's request of Ms. Del Greco and Dr. Goodwin. One thing that

I have noticed after being on this committee for 23 years is that what happens so often is that people say they are going to get things done, and they never get done.

So Mr. Meadows, in the spirit of efficiency and effectiveness, I think has made a very reasonable request that Ms. Del Greco and Dr. Goodwin get together so that we can get some of these items resolved. So I am going to call you all back in about two months maybe. I will figure it out. Because I am worried that this is going to go on and on, and in the meantime I am sure that we will be able to come up with some bipartisan solutions. But the American citizens are, I think, being placed in jeopardy as a result of a system that is not ready for prime time.

So we will call you all back. I hope that you all get together as soon as possible. Again, I say this because I have seen it over and over again, that we will be in the same position, or worse, in three years, five years, 10 years. By that time, so many citizens may have been subjected to something that they should not be.

With that, I call on——

Mr. MEADOWS. Mr. Chairman, I just want to say I appreciate your leadership on that and appreciate your follow up.

Chairman CUMMINGS. No problem.

I now call on the distinguished lady from Michigan, Ms. Lawrence.

Mrs. LAWRENCE. Thank you, Mr. Chair.

Dr. Romine, do you think that third-party testing is important for the safe deployment of facial recognition technology? And I want you to know that I sit on the Criminal Justice Appropriations Committee, and funding for NIST is something that I have a responsibility for. So I would really like the response to these questions.

Mr. ROMINE. I think independent assessment of new technologies, particularly if they are going to be used in certain ways, is an essential part and one of the things we are privileged to do as NIST.

Mrs. LAWRENCE. And how dependent are government agencies on NIST's findings? How dependent?

Mr. ROMINE. It is hard for me to assess that. I think we certainly have collaborative relationships with DHS, with FBI, with other Federal agencies. Part of our statutory requirement is working with other agencies on advancement of technologies and evaluation of technologies.

Mrs. LAWRENCE. Is there a way that we can move forward that you can do an assessment so that we would know when we are talking about the findings, which is a critical factor right now? Is there a way that we can move forward so that we can assess what is the role that you play, that is played by the third party?

Mr. ROMINE. With respect to facial recognition, we have ongoing evaluations on a rolling basis. So participants can submit algorithms at any time, and we continue to provide open, public, transparent evaluation methodologies so that everyone, Federal agencies and the public, the private sector, can see the results of our testing and make determinations on effectiveness of the algorithms.

Mrs. LAWRENCE. Through the Chair, I would like to review those.

Which organizations are currently equipped to accurately test new facial recognition technologies?

Mr. ROMINE. We are certainly equipped to do that at NIST. I don't have information about other entities that might also be equipped to do that.

Mrs. LAWRENCE. Do you believe that NIST currently has significant funding and resources to carry out your work as the standard bearer of the facial recognition industry?

Mr. ROMINE. Yes. We have sufficient resources today to be able to execute the program that we have in biometrics.

Mrs. LAWRENCE. To "carry out," that is the word that you are saying. As this is evolving and we are looking at the challenges, do you have enough funding for the R&D and for the checks and balances for you to be the standard bearer of the facial recognition industry? Nothing frustrates me more than for you to come before Congress and say I have everything I need, and then when you don't do the job, "Well, we didn't have the funding."

So I am asking this question, and I need you to be very honest with me.

Mr. ROMINE. I would make two remarks. One is we have a long track record of delivering high-quality evaluations in biometrics for nearly 60 years. The second part of it is it is a bit awkward for me in front of Congress, or any Federal official, to speak about funding levels. I will just make the comment that any research organization can do more with more, and I will leave it at that.

Mrs. LAWRENCE. Well, for me to do my job, I have to get past accurate, and you have to have a plan and directive.

I just want to ask if anyone on the panel wanted to comment on the organizations and the ability to accurately test new facial recognition technologies. Are there any comments from any of the others of you? No.

Thank you.

Chairman CUMMINGS. Thank you very much.

Ms. Miller?

Mrs. MILLER. Thank you, Chairman Cummings and Ranking Member Jordan.

And thank you all for being here today.

America has been a leader and an innovator in the technology sector. American companies have pioneered many of the technologies deployed around the world. However, as this sector continues to grow, we need to ensure that our government agencies are accurately deploying this technology within the bounds of law.

This past week I was in China and I saw facial recognition technology deployed on a massive scale from the moment I was getting ready to get on the airplane. There were cameras everywhere. Alibaba recently instituted a program where customers can "smile to pay" using facial recognition technology. I also saw cameras at street crossings that can pinpoint certain individuals who are breaking traffic laws. It was rather daunting to see the government shaming individuals so publicly, which is a stark contrast to what our privacy and our liberty is in America. I mean, they would flash your face right there.

Seeing this use of facial recognition technology in China poses many questions to the United States about the appropriate use of this technology.

Ms. Goodwin, Dr. Goodwin, what steps can our government take to ensure facial recognition technology is being deployed in a way that is accurate?

Ms. GOODWIN. Thank you for that question. I will always go back to the recommendations that we made when we did this work a few years ago that DOJ is still working through. Accuracy and transparency are key and vital to when we are talking about this technology, as well as just making certain that we are protecting privacy rights.

To go back to the recommendations, we want DOJ to pay more attention to the list sizes that they are testing. We want them to regularly assess whether the NGI-IPS, whether that information is accurate. We also want them to assess and have some understanding of whether the information that they are getting from their external partners is also accurate.

Mrs. MILLER. Thank you.

Ms. Del Greco, to your knowledge, has the FBI had any misidentifications of individuals when utilizing facial recognition technology?

Ms. DEL GRECO. I would like to go back to the statement by Dr. Goodwin. We did test all—since the last hearing in 2017, the FBI did test all of the list sizes and saw improvements in the accuracy. We conducted the Facial Recognition Vendor Test with NIST and are implementing a new algorithm, and we work continuously with our state and Federal and local partners on their use of our system. And we have also commissioned NIST to do a 2019 and onward—it is called an ongoing facial recognition test where we will be able to test the accuracy of the system yearly.

With regard to misidentification, I am not aware of any. Thank you.

Mrs. MILLER. Okay. Then basically my next question sort of falls right in line. Does the FBI have any plans to assess the rate of misidentifications generated by the Next-Generation Identification Interstate Photo System?

Ms. DEL GRECO. So the system was designed to return two or more candidates. We provide an investigative lead back to law enforcement, the law enforcement entity. We require training by law enforcement to follow the NGI Interstate Policy and Implementation Guide and the Facial Identification Scientific Working Group Standards. So anyone running a search through the NGI Interstate Photo System must comply with the policies and standards, and they are audited by our FBI triennially.

Mrs. MILLER. Can you discuss the regulations in place that allow for an agent to utilize facial recognition technology and how strictly these regulations are enforced?

Ms. DEL GRECO. I do know that for the FBI FACE Services Unit, an FBI field office must have an open assessment or an active investigation, and they must follow the Attorney General guidelines associated with that for us to be able to receive a probe photo from them and then submit the probe photo for a search.

Mrs. MILLER. Okay. And, Dr. Goodwin, to your knowledge, has the FBI been adhering to these regulations?

Ms. GOODWIN. We are working very closely with the FBI. If I could go back to something Ms. Del Greco said earlier, the testing that they are currently doing, the new information that they are providing, until we see that, we won't be closing our recommendations. We need to make certain that they are meeting the recommendations as we have put forward to them.

Mrs. MILLER. Okay, thank you.

I yield back my time.

Chairman CUMMINGS. Mr. Gomez?

Mr. GOMEZ. Thank you, Mr. Chairman.

In the history of this country, we have always had this debate and this goal of trying to balance security with liberty. But in the era of facial recognition, I feel that we are stumbling into the future without really understanding how much liberty we are giving up for how much security. And it is really with that understanding that we have to set up guidelines that really dictate the use of this technology. So that is where my approach comes from.

I have a lot of concerns regarding the false-positive rate of the technology, racial bias in the technology, gender bias, and even during—this is Pride Month, June is Pride Month. I think about the transgender and non-binary communities, and we have seen reports that show that black women are more likely to be misidentified than any other group. So when you layer on top of that the transgender, non-binary, black individual, what happens to those results?

Mr. Romine, have you seen any data when it comes to the LGBTQ community, specifically the transgender community?

Mr. ROMINE. We haven't done an analysis of accuracy rates for the transgender community. I am not sure how we would obtain the relevant data that we would use to do that, but I am aware of—I have been made aware of concerns in the transgender community about the potential for problematic use here.

Mr. GOMEZ. Okay, I appreciate that. A lot of this also revolves around training. I know that NIST has pointed out and indicated that people are likely to believe computer-generated results, and those who aren't specially trained in face recognition have problems in identifying people they don't know, even if they perform face identifications as part of their work. So I am kind of keeping that in mind with the questions I am about to ask.

First, Ms. Del Greco, what is the confidence level the FBI uses when it comes to running the program for the matches? Is it 80 percent? Is it 85 percent? Is it 95 percent? Is it 99 percent?

Ms. DEL GRECO. Our quoted accuracy rate—and we don't have matches. Let me clarify that first, sir. It is an investigative lead. It is two or more candidates. Our system is not built to respond to one response. Currently we have an 85 percent accuracy rate, although since the last hearing we——

Mr. GOMEZ. That is not what I am asking. I am asking when you run the program, is it set to a high level that it needs to be accurate, to a 95 percent confidence level that the computer recognizes that this individual is 95 percent likely to be this person, or is it

80 percent? Like Amazon sells their program at 80 percent default. What do you guys run your program at?

Ms. DEL GRECO. Because we don't conduct an identification match, we don't look at that, sir. We do have an accuracy rate that we rely on, and we are currently implementing the new NIST Vendor Recognition Test results at 99.12 percent at a Rank 1, and it is 99.72 at a Rank 50. Those are the new—that is the new algorithm. But because it is not a true identification, we don't print that.

Mr. GOMEZ. Okay. How does the FBI combat the human tendency to trust computer-generated results?

Ms. DEL GRECO. Well, through the testing with NIST for sure, and then we also use other agencies and entities, universities, to provide testing results to us.

Mr. GOMEZ. Do you train FBI personnel to perform facial comparisons of persons that are unknown to them?

Ms. DEL GRECO. We receive probe photos from an active investigation from the FBI field office, an FBI agent, and they process that probe photo against our mug shot repository and receive a candidate back, and they are trained to evaluate.

Mr. GOMEZ. Okay. So does the FBI train personnel on the potential inaccuracies and biases of facial recognition algorithms?

Ms. DEL GRECO. Bias for the algorithm?

Mr. GOMEZ. Yes.

Ms. DEL GRECO. No, sir.

Mr. GOMEZ. And why is that?

Ms. DEL GRECO. Well, I think the employees—I mean, our system doesn't look at skin tone and features. It is a mathematical computation that comes back, and they are to look at the mathematical

[inaudible] of the face.

Mr. GOMEZ. Okay. I understand that you are basically describing facial recognition technology, but outside studies have shown that there is a bias when it comes to certain populations, that the error rate was a lot higher. Were you aware that the ACLU conducted a match of different Members of Congress at an 80 percent confidence interval level, and Members of Congress, including myself, were mismatched positively with mug shot photos?

Ms. DEL GRECO. So the technology you are referencing to is an identification, and that is a match. We do not do that.

Mr. GOMEZ. So you do broader.

Ms. DEL GRECO. We do two to 50 candidates back. Our employees look at two candidates or more. We do not look at one-to-one match. It is not a match.

Mr. GOMEZ. Okay. The FBI publishes that it trains third parties in a manner consistent with the guideline and recommendations outlined by the Facial Identification Scientific Working Group. The Facial Identification Scientific Working Group does not endorse a standard certified body of facial comparison. To compare, the ten print certification exists for personnel that analyze fingerprints. These programs require hours of training before a person can be certified. Since there is no formal certification process that the Working Group endorses, what standards does the FBI require of personnel that conduct facial analysis?

Chairman CUMMINGS. The gentleman's time has expired.

Ms. DEL GRECO. So we did publish, and our own employees in the FACE Services have to comply with as well. We require all law enforcement entities that have access to the Interstate Photo System to follow the FBI's Policy and Implementation Guide and the Standards. They have to follow both.

Chairman CUMMINGS. The gentleman's time has expired. Thank you very much.

Mr. GOMEZ. Thank you, Mr. Chairman.

Chairman CUMMINGS. Ms. Pressley?

Ms. PRESSLEY. Thank you, Mr. Chairman.

It has been abundantly clear that facial recognition technology is flawed by design, unlawfully producing false matches due to algorithmic bias, including to everyday Americans, and in fact even Members of Congress, which Representative Gomez was one of those. He was just speaking to that. And there is growing and, I do believe, credible concern over the unauthorized use of this technology in public spaces such as airports, schools, and courthouses. These systems can certainly be subject to misuse and abuse by law enforcement. And we know that this technology is often used without consent.

In that there are no real safeguards, there are no guardrails here, this is not fully developed, I just want to take a moment to say that I appreciate the leadership of the city of Summerville in my district, the Massachusetts Seventh, and Counselor Ben Campion and Mary Jo Corditone, who have passed a moratorium on this surveillance and on this software because of the fact that it is not developed and there are just no safeguards and no guardrails.

Much of my line of questioning has already been asked, but I do just want to pick up on a couple of things in the space of consent because I wanted to just get some accuracy questions and just better understand for the purposes of the record here.

Mr. Gould, do you keep data on how many people opt out of use for the facial recognition technology?

Mr. GOULD. Ma'am, I am not aware that we are actually collecting data on people who choose not to participate. I don't think we are collecting it. No, ma'am.

Ms. PRESSLEY. Okay. And so you have no idea how many people have opted out of previous TSA facial recognition pilot programs?

Mr. GOULD. No, ma'am.

Ms. PRESSLEY. Okay. Do you know how many passengers were notified of TSA's use of facial recognition technology?

Mr. GOULD. Ma'am, the notification at the airport consists of signage and also verbal instructions from the officers. So if they are in a lane where facial recognition technology is being piloted, I would say that 100 percent of the people are being made aware that it is being used. And they actually have to assume a suitable pose to actually have the camera capture their image.

Ms. PRESSLEY. So again, if this is based on signage, which in many ways can be arbitrary, how are folks even aware of the option to opt out, other than signage? And then how do they opt out?

Mr. GOULD. It is signage. It is announced. "If you would like to have your picture taken for your identification, please stand right

here. Otherwise, let us see your credential, your hand-carried identification."

Ms. PRESSLEY. Okay. And is that communicated in multiple languages?

Mr. GOULD. For the purposes of the pilot, ma'am, it has not been communicated in multiple languages.

Ms. PRESSLEY. Okay. Again, just for the purposes of the record, I guess I over-spoke based on my own desires that the municipality in my district, the Massachusetts Seventh, Summerville passed an ordinance to ban but has not yet passed a moratorium, so I just wanted to correct that for the purposes of the record.

Let me just for a moment just get back into some questions regarding government benchmarking for facial recognition. Dr. Romine or Dr. Goodwin, are you aware of how many government agencies use or possess facial recognition technology?

Dr. Romine or Dr. Goodwin, or anyone.

Mr. ROMINE. I don't know that answer.

Ms. GOODWIN. Nor do I. I also do want to put in front of everyone, the GAO does have ongoing work right now looking at the use of FRT at CBP and at TSA. So we will be following up on the information here.

Ms. PRESSLEY. Okay. So is there a stabilizing, like a comparative sort of benchmark as to the accuracy of these programs and how they compare with other programs?

Ms. GOODWIN. We are not aware of that as of yet.

Ms. PRESSLEY. Okay. Did NIST present any red flags to agencies about inaccuracies in any particular system used by a government agency that you are aware of?

Mr. ROMINE. NIST doesn't interpret the scientific data in terms of red flags. Instead, we just ensure that everyone who is using facial recognition technology has access to the scientific data that we publish openly about the performance of the algorithms that have been voluntarily submitted to our program.

Ms. PRESSLEY. Okay. All right. I think that is it for me, for now. I yield. Thank you.

Chairman CUMMINGS. Let me just ask you this, Dr. Goodwin. You said there is ongoing work. What is happening there?

Ms. GOODWIN. So we have ongoing work at the request of both the Senate and the House Homeland Committees to look at the use of face recognition technology at DHS, and in particular TSA and CBP. We also have ongoing work looking at the commercial uses of face recognition technology.

And if I could just kind of circle back to Congresswoman Pressley's comment about consent, there is the Senate bill that will look at consent, but it only looks at consent from the standpoint of commercial usage, not Federal usage. So we have those ongoing jobs. And then GAO does have a request in to look at face recognition technology across the rest of law enforcement.

Chairman CUMMINGS. Well, going back to Ms. Pressley's questions about the whole idea of language, do you all feel comfortable? I mean, I assume that you have looked at TSA already, right?

Ms. GOODWIN. We are just starting that engagement, so we haven't——

Chairman CUMMINGS. So you haven't looked at the pilot program.

Ms. GOODWIN. Not as of yet, but I imagine that will be part of what we examine. But that engagement, that work just started at GAO.

Chairman CUMMINGS. And one of the things I am hoping that you will look at is that whole question. You know, people are in a hurry. They are trying to get to where they have to go. A lot of people don't even know what facial recognition is. They don't have a clue. And then if you have a language problem, that is even more, Mr. Gould. It is something to consider. Have you all thought about that?

Mr. GOULD. Yes, sir. I was remiss when I answered the question before. One of the reasons we are doing these pilots is to really assess the efficiency of how we communicate with passengers, can we do it better, can the signage be better, multiple languages in certain areas, is that something we should be looking at. All that will be assessed with respect to these pilots before making a decision moving forward.

Chairman CUMMINGS. Ms. Tlaib?

Ms. TLAIB. Thank you, Mr. Chairman. I have to tell you—and through the Chairman, I hope this is okay—this stuff freaks me out. I am a little freaked out by facial recognition, Mr. Chairman. I hope that is okay, I can say that.

Chairman CUMMINGS. Yes, that is okay.

Ms. TLAIB. Thank you.

My residents in Michigan's 13th congressional District have been subjected to increased surveillance and over-policing for decades. Currently, the city of Detroit rolled out a real-time video surveillance program called Project Green Light in 2016 to monitor crime at late-night businesses like gas stations and liquor stores. But now the system has expanded to over 500 locations, including parks, churches, schools, women's clinics, addiction treatment centers, and now public housing buildings. Without notice or public comments from residents, the Detroit Police Department added facial recognition technology to Project Green Light, which means Detroit Police Department has the ability to locate anyone who has a Michigan driver's license or an arrest record in real time using video cameras mounted across the city in a data base of over 50 million photos.

In January 2019, reports emerged that FBI had begun piloting the use of Amazon Rekognition, Amazon's controversial software that can match faces in real-time video, similar to Project Green Light. Rekognition, like real-time facial surveillance programs, has dangerously high error rates for women of color as compared to white males. In the 13th congressional District, residents will disproportionately bear the harms of facial recognition misidentification.

So, Ms. Del Greco, what policies does the FBI have in place regarding the use of real-time facial recognition technology? I heard claims that you all are not using it, but there is a pilot program; correct?

Ms. DEL GRECO. No, there is not. For the Amazon Rekognition software, to the best of my knowledge and verified before I came

today, the FBI does not have a contract with Amazon for their Rekognition software. We do not perform real-time surveillance.

Ms. TLAIB. Through the Chair, if I may, if you can produce that documentation and that information to our committee, I would really greatly appreciate that.

Ms. DEL GRECO. We will do so.

Ms. TLAIB. Now, can you explain how the FBI—so the FBI is not currently using Amazon Rekognition at all.

Ms. DEL GRECO. We are not.

Ms. TLAIB. Good. So in March 2017, NIST released a report on accuracy of facial recognition systems when applied to individuals captured in real-time video footage. The report found significantly higher error rates for real-time use of Rekognition, with accuracy rates as low as 60 percent.

So, Dr. Romine, do you think that the use of real-time facial recognition technology is ready for law enforcement usage?

Mr. ROMINE. That is a judgment that NIST is not prepared to make. That is a policy judgment that should be predicated on the best available scientific data, which is our position.

Ms. TLAIB. Well, what does your scientific data say?

Mr. ROMINE. The scientific data verifies that facial recognition accuracy is highly dependent on image quality and on the presence of injuries. Both of those things can affect the ability to have accurate——

Ms. TLAIB. So is there any viable solution to improving the real-time capabilities?

Mr. ROMINE. I can't predict how accurate the systems will be in the future as they continue to develop. Currently, systems that use facial images that are not in profile or that are not straight on, like mug shot images, or facial images that are indistinct or blurred, have a much lower ability to match.

Ms. TLAIB. Dr. Goodwin, do you have any information about the inaccuracies—and I know that you all had several recommendations, but can you talk a little bit more about my question in regards to is this fixable?

Ms. GOODWIN. So, in regards to your question about the Amazon Rekognition technology, that was not something that we looked at for the purposes of our report, so I won't be able to speak to that.

Ms. TLAIB. But in regards to, right now, the use of facial recognition accuracy, you all had six recommendations about transparency and so forth, but I was just talking to some of my colleagues, and how do you fix something like this when you dump so many innocent people into a data base? I mean, the numbers are 411 million. I think I heard from you 600 million people are now in this data base that is being used for criminal justice purposes, which I am not sure what is the definition of that.

Ms. GOODWIN. So, I will kind of start a little bit at the beginning. So for the NGI-IPS, there are 36 million photos in the criminal part of that. There are 21 million photos for the civil part of that. And then as you look across all of the searchable data bases or repositories that FACE has access to, that is over 600 million. So that is what I was talking about earlier.

The recommendations that we made, those three recommendations that we made related to accuracy, we feel like this would go

a long way to helping DOJ better ensure that the data that they are collecting, the way they are using the information, that that is accurate. As of yet, as you have heard, DOJ has yet to close those recommendations, and we will work very closely with them to get those closed because the issues around privacy and accuracy are very important, and they are vitally important when you are talking about using this technology.

Ms. TLAIB. Thank you.

Mr. Chairman, through you, if it is possible, this is very important to my district and to others, if we can get some follow up and confirmation that indeed the current administration does not have any pilot program going on with Amazon Rekognition program?

Chairman CUMMINGS. Thank you very much, Ms. Tlaib. What we will do—I don't know if you heard me earlier—we are going to bring folks back in six weeks to two months, somewhere in that area, and I am hoping that before then they will have those questions resolved. But definitely we will check back then. All right?

Ms. Ocasio-Cortez?

Ms. OCASIO-CORTEZ. Thank you, Mr. Chair.

In the Fourth Amendment, our founding fathers endowed with us "the right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures." The Fourth Amendment guarantees us that these areas shall not be unreasonably intruded upon with most searches founded upon a warrant. And over the last few weeks we have been hearing, whether from the private sector or the public, we have heard about facial recognition technology being used in airports, protests, being purchased off of social media, et cetera.

Ms. Del Greco, you are with the FBI. Does the FBI ever obtain warrants before deploying the use of facial recognition technology?

Ms. DEL GRECO. The criminal mug shots are searched by our law enforcement partners, and all photos are collected pursuant to an arrest with the criminal ten print fingerprint.

Ms. OCASIO-CORTEZ. And in use of facial recognition, it is beyond just the search of the criminal data base but scanning a person's face I would say is akin to searching their face in order to match it to a data base. Does the FBI ever obtain a warrant to search someone's face using facial recognition?

Ms. DEL GRECO. We do not do real-time searching. We do not.

Ms. OCASIO-CORTEZ. Okay. Do you require your external partners to obtain a warrant?

Ms. DEL GRECO. I mean, they must do so with a criminal law enforcement interest.

Ms. OCASIO-CORTEZ. Does the FBI use any information from any other agency with respect to facial recognition?

Ms. DEL GRECO. We share our records with other Federal agencies with regard to law enforcement purposes.

Ms. OCASIO-CORTEZ. In our May 22 hearing, Chairman Cummings stated that he was present at the 2015 Baltimore protests following the death of Freddie Gray. At those protests the Baltimore County Police Department allegedly used facial recognition technology to identify and arrest certain citizens present at the protest exercising their First Amendment rights.

Ms. Del Greco, has the FBI ever used facial recognition deployed at or near a protest, political rally, school, hospital, courthouse, or any other sensitive location?

Ms. DEL GRECO. No, we have not.

Ms. OCASIO-CORTEZ. And do you think that the generalized facial surveillance should be permissible? Do you think that that undermines the First Amendment?

Ms. DEL GRECO. I do think that protecting the American people is extremely important to us. The FBI absolutely wants the best, most fair system. We want to make sure that we are following the guidelines, process, protocols, and standards that we put in place for law enforcement.

Ms. OCASIO-CORTEZ. Okay, thank you.

Mr. Gould, you are with the TSA. The TSA has outlined proposals to collaborate with private companies, including Delta and Jet Blue, to develop and implement their facial recognition search systems. Is this correct?

Mr. GOULD. Ma'am, we have issued a security program amendment to Delta to allow them to use biometric identification at their bag drop. In terms of partnering with them to develop the back-end matching system, that is something that we are solely engaged with CBP on.

Ms. OCASIO-CORTEZ. And the bag drop, those are the computers that folks check in and get their boarding pass from?

Mr. GOULD. That would be the—I would use the term "kiosk" for that.

Ms. OCASIO-CORTEZ. The kiosk.

Mr. GOULD. Delta uses that technology at their kiosk. TSA has no equity there. That is solely to verify that passengers have a reservation with Delta. Where we have equity is at our checkpoint, and also at the bag drop, where we are required to ensure that the passengers match to their bag.

Ms. OCASIO-CORTEZ. Do individuals know that that is happening, and do they provide explicit consent? Is it opt in?

Mr. GOULD. Passengers have the opportunity to not participate.

Ms. OCASIO-CORTEZ. So it is opt out, but not opt in.

Mr. GOULD. It is. Yes, ma'am.

Ms. OCASIO-CORTEZ. So it is possible that Jet Blue and Delta are working with the TSA to capture photos of passengers' faces without their explicit opt-in consent.

Mr. GOULD. Ma'am, I was down in Atlanta last week and watched the Delta check-in process, the bag drop process, and it was very clear while I was down there that passengers were afforded the opportunity, if you would like to use facial capture for identification, please stand in front of the camera and we will do so. There was no automatic capture of passengers or anything like that.

Ms. OCASIO-CORTEZ. And this capture is not saved in any way; correct?

Mr. GOULD. No, ma'am. The camera captures the image. The image is encrypted. It is sent to the TVS matching system, which is what CBP uses, solely for the purpose of match, and then that match result is sent back to the operator.

Ms. OCASIO-CORTEZ. Is that captured image destroyed?

Mr. GOULD. It is not retained at all. No, ma'am.

Ms. OCASIO-CORTEZ. So it is sent, but it is not retained.

Mr. GOULD. It is not retained on the camera. No, ma'am.

Ms. OCASIO-CORTEZ. Okay. Could these companies potentially be using any part of this process to either capture the algorithm or data?

Mr. GOULD. No, ma'am. I don't see that happening currently with the pilots that we are doing right now.

Ms. OCASIO-CORTEZ. Okay, thank you very much.

I yield back to the Chair.

Chairman CUMMINGS. Thank you very much.

Mr. Sarbanes?

Mr. SARBANES. Thank you very much, Mr. Chairman.

When we had our hearing on May 22 in this committee, there was an MIT researcher, Joy Buolamwini, who was testifying about datasets that NIST uses, and that they may not adequately test for the full range of diversity present in the U.S. population. She said, "In evaluating benchmark datasets from organizations like NIST, I found some surprising imbalances. One prominent NIST dataset was 75 percent male and 80 percent lighter skinned, what I like to call a 'pale male' dataset."

So, Dr. Romine, can you discuss how representative datasets are when it comes to race, gender, and age?

Mr. ROMINE. Sure. The data that we obtain is from multiple sources. The largest amount of data that we get—first I need to make a distinction between data that we are releasing as part of the ability for vendors to determine whether they are able to submit their algorithms to our system, to our evaluation process. So we provide them with data for that.

The rest of our data, the vast majority of it, is sequestered. It is not made public. It is solely for the purposes of evaluation. Most of that data is FBI image data that we sequester and protect from release. There is some other image data related to Creative Commons, to images that we have received with full institutional review that involves permissions, and then also deceased datasets.

In all cases, if you look at the full suite of data, it is true that it is not representative of the population as a whole. However, we have a large enough dataset that our evaluation capabilities can be statistically analyzed to determine demographic effects of race, age, or sex. And we are in the process of doing that now and will release that report in the fall.

Mr. SARBANES. So I gather that since the last hearing you have been testing for differential error rates on the facial recognition systems between races and genders. Can you talk a little bit more about the error rates of the algorithms that you tested between different races and genders?

Mr. ROMINE. Sure. I can say a little of preliminary information, but I want to stress that the full statistical analysis, the rigorous analysis, is not completed yet. The report will be released in the fall that outlines the full conclusions that we have with regard to effects, demographic effects, broadly speaking.

We can say that there are still remaining differences even with the extraordinary advances in the algorithms over the last five years. There are still differences remaining that we can detect. We

don't yet know whether those differences—whether it is with regard to race, sex, or age—are significant. We don't know yet until we have completed that analysis.

Mr. SARBANES. So you understand the concern. There are at least two levels of analysis that are of concern here today. One is the threshold question of whether we like or don't like this technology given the general threat that it can pose to civil liberties. The second theme is whether recognizing that the technology is barreling ahead anyhow and is being adopted and applied increasingly across many different platforms, let's say, and uses, whether it is being developed in a way that ensures that when it is used, it is not being used in a discriminatory fashion, it is not being applied unfairly, et cetera. And that depends on the algorithms being developed in a way that is respectful of accurate data, and we are not there yet, as I understand it. So it just increases the anxiety level.

So we are going to be paying a lot of attention. I am glad the Chairman is going to have you all come back, because I think he is right that this is sort of a moving target here. We are going to be paying a lot of attention to how the data gets digested and how the algorithms that flow from that data are being applied, whether they are accurate and so forth.

So we appreciate your testimony, but obviously this is not the end of the inquiry.

With that, I yield back.

Chairman CUMMINGS. Mr. Sarbanes, a while ago we were told that the basis for a lot of these agreements between the FBI and the states were—well, the authorization and regulations, whatever, were put together before facial technology came about, if you want to talk about the moving target. So it wasn't even anticipating this, and we still haven't caught up. That is part of the problem.

Thank you very much.

Mr. Jordan?

Mr. JORDAN. Thank you. Thank you, Mr. Chairman.

I want to thank our witnesses for being here today. I appreciate the time and the expertise that you brought to this important hearing. I think you understand that from both sides of the aisle there is a real concern.

Ms. Del Greco, I appreciate you being here. I know you had to answer a lot of questions. But I hope you understand how serious everyone is on this committee with this issue.

I think you have to understand the framework. I mean, you talked about strict standards in place. There were strict standards in place, at least people from our side of the aisle view it this way, strict standards in place on how people go to the FISA court and get information and put information in front of the FISA court. The Attorney General of the United States has tapped U.S. Attorney John Durham to look at potential spying done by the FBI of one Presidential campaign.

So this is the context and the framework that many on our side see this happening, and it is happening when GAO—not Jim Jordan, not Republicans—GAO—Dr. Goodwin said that when you guys started this, started using this, you didn't follow the E-Government law, you didn't do privacy impact assessments like you are supposed to, you didn't provide timely notice, didn't conduct proper

testing, and didn't check the accuracy of the state systems that you were going to interact with.

So that is the backdrop, that is the framework. So when Republicans talk about we are concerned and working with Democrats—and I really do appreciate the Chairman's focus on two hearings, and now a third hearing, and looking at legislation that we may attempt to pass here. This is the framework. So I hope you will tell the folks back at the FBI, we appreciate the great work that FBI agents do every single day protecting our country and stopping bad things from happening and finding bad people who did bad things, but the framework and the context is very serious, and that is why we come at it with the intensity that I think you have seen both two weeks ago in that hearing and in today's hearing.

So again, Mr. Chairman, thank you for your leadership on this, and I would thank our witnesses again for being here.

Chairman CUMMINGS. I too want to thank the witnesses for being here for almost three hours. We really do appreciate your testimony.

Of all the issues that we have been dealing with, this probably will receive the most intense scrutiny of them all. The Ranking Member referred to the fact that we are bringing you all back, but we also have two subcommittees that are also looking into this because we want to get it right. It is just that important, and so I thank you.

Without objection, the following shall be a part of the hearing record: Face Recognition Performance, Role of Demographic Information, scientific study dated December 6, 2012; Faceoff, Law Enforcement Use of Face Recognition Technology, white paper by the Electronic Frontier Foundation; GAO Priority Open Recommendations, Department of Justice letter to AG Barr and GAO; Ongoing Face Recognition Vendor Tests, Part I Verification, NIST report, NIST; Ongoing Face Recognition Vendor Tests, Part II, NIST report; Face and Video Evaluation, Face Recognition of Non-Cooperative Subjects, NIST report; coalition letter calling for a Federal moratorium on face recognition, coalition letter; and the coalition of privacy, civil liberties, civil rights, and investor and faith groups, including the ACLU, Georgetown Law, LGBT Technology Partnership, and the NAACP.

Chairman CUMMINGS. I want to thank again our witnesses for being here today.

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 would ask that our witnesses please respond as promptly as possible.

With that, this hearing is adjourned.

[Whereupon, at 12:50 p.m., the committee was adjourned.]