AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

LAW ENFORCEMENT'S USE OF FACIAL RECOGNITION TECHNOLOGY

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

MARCH 22, 2017

Serial No. 115–52

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://oversight.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

28–689 PDF WASHINGTON : 2018

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

Jason Chaffetz, Utah, *Chairman*

John J. Duncan, Jr., Tennessee
Darrell E. Issa, California
Jim Jordan, Ohio
Mark Sanford, South Carolina
Justin Amash, Michigan
Paul A. Gosar, Arizona
Scott DesJarlais, Tennessee
Trey Gowdy, South Carolina
Blake Farenthold, Texas
Virginia Foxx, North Carolina
Thomas Massie, Kentucky
Mark Meadows, North Carolina
Ron DeSantis, Florida
Dennis A. Ross, Florida
Mark Walker, North Carolina
Rod Blum, Iowa
Jody B. Hice, Georgia
Steve Russell, Oklahoma
Glenn Grothman, Wisconsin
Will Hurd, Texas
Gary J. Palmer, Alabama
James Comer, Kentucky
Paul Mitchell, Michigan

Elijah E. Cummings, Maryland, *Ranking Minority Member*
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
Robin L. Kelly, Illinois
Brenda L. Lawrence, Michigan
Bonnie Watson Coleman, New Jersey
Stacey E. Plaskett, Virgin Islands
Val Butler Demings, Florida
Raja Krishnamoorthi, Illinois
Jamie Raskin, Maryland
Peter Welch, Vermont
Matt Cartwright, Pennsylvania
Mark DeSaulnier, California
John P. Sarbanes, Maryland

JONATHAN SKLADANY, *Staff Director*
WILLIAM MCKENNA, *General Counsel*
TROY STOCK, *Information Technology Subcommittee Staff Director*
SEAN BREBBIA, *Senior Counsel*
SHARON CASEY, *Deputy Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

CONTENTS

Page

Hearing held on March 22, 2017 1

WITNESSES

Kimberly Del Greco, Deputy Assistant Director of Criminal Justice Information Services Division, Federal Bureau of Investigation
- Oral Statement 5
- Written Statement 7

Diana Maurer, Director, Homeland Security and Justice Issues, U.S. Government Accountability Office
- Oral Statement 12
- Written Statement 14

Charles Romine, Ph.D., Director of Information Technology Lab, National Institute of Standards and Technology
- Oral Statement 36
- Written Statement 38

Alvaro Bedoya, Executive Director, Center on Privacy & Technology, Georgetown Law
- Oral Statement 45
- Written Statement 47

Benji Hutchinson, Senior Director, NEC Corporation of America On behalf of The International Biometrics + Identity Association
- Oral Statement 64
- Written Statement 66

Jennifer Lynch, Senior Staff Attorney, Electronic Frontier Foundation
- Oral Statement 76
- Written Statement 78

APPENDIX

Letter of June 23, 2016, Requesting Congressional Oversight, submitted by Mr. Chaffetz 132

Letter of September 6, 2016, to Mr. James B. Corney, Federal Bureau of lnvestigation, submitted by Mr. Chaffetz 138

Response from Dr. Romine, NIST, to Questions for the Record 141

LAW ENFORCEMENT'S USE OF FACIAL RECOGNITION TECHNOLOGY

Wednesday, March 22, 2017

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

The committee met, pursuant to call, at 9:30 a.m., in Room 2154, Rayburn House Office Building, Hon. Jason Chaffetz [chairman of the committee] presiding.

Present: Representatives Chaffetz, Duncan, Jordan, Gosar, Foxx, DeSantis, Ross, Grothman, Palmer, Comer, Mitchell, Cummings, Maloney, Norton, Clay, Lynch, Connolly, Kelly, and Krishnamoorthi.

Chairman CHAFFETZ. The Committee on Oversight and Government Reform will come to order.

Without objection, the chair is authorized to declare a recess at any time.

We have an important hearing today about law enforcement's use of facial recognition technology. It's exciting technology. The world of technology offers us a lot of opportunities, but just because we can doesn't mean we necessarily should, and so there are a number of things that we need to have discussions about and try to figure out and tackle as a society.

And this is one in a series of things that we're going to be discussing in this year and next as technology brings us to new frontiers and new paths and new things that we need to dive into and look at, because, again, while there's a lot of excitement and a lot of opportunity, there's also opportunities to have it misused or overused or create a whole other set of problems that maybe our Nation and our society and our generation have not yet dealt with.

This happens to be one of those types of technologies. Facial recognition technology, it is exciting what can be done, but we have to look at how this affects law enforcement and our rights as Americans, particularly suspicion-less Americans and our right for privacy.

The days of the old Sherlock Holmes dusting for fingerprints and looking for clues, they're being replaced by algorithms and software scanning millions of images at unprecedented speeds to match a face to a name. However, like many technologies used in the wrong hands or without appropriate parameters, it is ripe for abuse; therefore, the oversight of the use of this technology is essential.

Until recently, fingerprint analysis was the most widely used biometric technology for positively identifying arrestees and linking them to previous criminal history. In 2010, the FBI began replac-

ing its legacy fingerprint database with an updated database that incorporates advancements in biometrics, such as facial recognition, called the Next Generation Identification, or NGI. This is a database with an estimated cost of $1.2 billion. The FBI claims the NGI system, "brought the FBI's biometric identification system and criminal history information to the next level."

Unfortunately, the FBI failed—failed—to fulfill its statutory duty to inform the public of this new next-level capability and used facial recognition technology for 5 years without publishing the required Privacy Impact Assessment, as required by law. Further, agreements are in place with 18 States that allow the FBI to request those States search their databases, including driver's license databases, using facial recognition technology.

And if we have a graphic, let me have them put that up here, if we could. Just to give you—those States in the dark blue are the ones that have various types of relationships with the FBI. Those in the light blue do not have those types of relationships. But you can kind of get a sense of where the Nation is going and how States are entering into these memorandums of understanding.

You can take the graphic down.

To be clear, this is a database or a network of databases comprised primarily of law-abiding Americans. Eighty percent of the photos in the FBI's facial recognition network are of noncriminal entries, each of the photos from driver's licenses—they come from places like driver's licenses, passports, and whatnot.

It would be one thing if facial recognition technology were perfect or near perfect, but it clearly is not. Facial recognition technology does make mistakes. For example, in a test the FBI conducted prior to deploying NGI, roughly one in seven searches of the FBI system returned a list of entirely innocent candidates, even though the actual target was in the database.

I also have concerns about studies suggesting facial recognition technology may have been unintended—have unintended racial, gender, or age bias or deficiencies. Any technology biases or weaknesses correlating to race, gender, and age raise some serious concerns and need to be widely known and contemplated by law enforcement, legislative bodies, and the judiciary.

Facial recognition technology is a powerful tool for law enforcement that can be used to protect people, their property, our borders, and our Nation. The private sector may use technology to control access to sensitive information, protect financial transactions, verify time and attendance, and prevent fraud or identity theft, among other uses.

But it can also be used by bad actors to harass or stalk individuals. It can be used in a way that chills free speech and free association by targeting people attending certain political meetings, protests, churches, or other types of places in the public.

Perhaps most concerning is the prospect of its real-time use to track people's location throughout the day, a potential use that would fundamentally change what it means to live in a free society. For those reasons and others, we must conduct proper oversight of this emerging technology. I appreciate the witnesses and what they bring here.

One of the things that we're going to also talk about today is, what does it mean when you populate the database? If the FBI could have its way, the best I can understand it, they would put everybody's face in one database or a whole series of databases. And so what does that mean? I guess, if it's in a secure lockbox that nobody else can look at except the FBI, some people would argue that's a good thing. But we've seen the FBI, most recently, can't even keep the 702 information private and secure.

I don't trust the Federal Government. I don't believe that there is such a thing where they can keep all of this information locked down and secure. Does anybody really trust and believe that they can create this massive database? Imagine how valuable that database is going to be if they had the facial recognition of every single American in their system. And then you could just go online and you could start figuring out exactly who is walking in your door. Some companies are actually using this type of technology. They know who you are before you walk in the door. And what does that mean if this information were to get into the wrong hands? So it poses a number of issues and challenges.

I'd now like to yield such time as he may consume to Mr. Jordan of Ohio.

Mr. JORDAN. Thank you, Mr. Chairman, and I'll be real brief. I just wanted to thank you for this hearing and your continued focus on privacy, particularly in this digital age which we find ourselves a part of, and announce to the committee that I'm pleased to be working with, on a bipartisan basis, Congressman Lieu on developing a framework for facial recognition technology, how that is appropriate, what we hope is model legislation, frankly working with some of the good folks on our panel, like Mr. Bedoya, to develop that information.

Understand the context. We learned that several Federal agencies used StingRay technology to conduct surveillance on Americans without a probable cause warrant. During that hearing, we also learned that the IRS several times used that same technology without a probable cause warrant, the same IRS that targeted people for exercising their First Amendment liberties, targeted people for their political beliefs.

That is the context we find ourselves in today, and now we have this system in all those States that the chairman just put up. This is a critical issue at the appropriate time. And so I just, again, wanted to thank the chairman and look forward to hearing from our witnesses today, and appreciate this hearing and just how critically important it is to Americans' First Amendment and Fourth Amendment liberties.

With that, I yield back.

Chairman CHAFFETZ. I thank the gentleman.

Again, one of the key questions, seminal questions, before us is, is it the right public policy to populate a database with everybody's face in it, even the suspicion-less Americans? Is that the American way? Or—or—should they maybe be building a database of known criminal elements, people who maybe earned it, rather than the suspicion-less people who went in to get their driver's license and didn't know that they were also giving that information to the Fed-

eral Government and that the Federal Government would be using it for who knows what?

And as Mr. Jordan pointed out, there is technology, more—almost 500 units of these cell phone simulators, where the government is using cell phone simulators to track suspicion-less Americans in their very geolocation and their very location. You combine that with facial recognition technology, where somebody's walking down the street and they can be recognized and identified into a database that has been built by the FBI; it does pose questions.

The technology will also show us, the statistical data will show us the bigger the database, the more difficult it is for the facial recognition technology to get it right. If the database was smaller to known criminals, wanted criminals, people that are here illegally, maybe those are the types of things that we should be focused on, as opposed to everybody. And that's one of the questions that—and why we have a distinguished panel today.

So I will hold the record open for 5 legislative days for members who would like to submit their written statement.

And I would now like to recognize our panel of witnesses. We're pleased to welcome Ms. Kimberly Del Greco, who is the Deputy Assistant Director of the Criminal Justice Information Services Division of the Federal Bureau of Investigation. We do appreciate you being here.

We also have Diana Maurer—did I pronounce that right? I hope so—Director for Homeland Security and Justice Issues at the United States Government Accountability Office. She was just in Judiciary yesterday. So we appreciate the quick turnaround in being here again today.

Mr. Charles Romine, the Director of Information Technology Lab at the National Institute of Standards and Technology.

Mr. Alvaro Bedoya is the executive director for the Center of Privacy & Technology at Georgetown Law. Great mind and thought on this topic, and we appreciate you being here, sir.

Mr. Benji Hutchinson, senior director for the NEC Corporation of America, testifying on behalf of the International Biometrics + Identity Association.

And Ms. Jennifer Lynch, senior staff attorney for the Electronic Frontier Foundation. We thank you for being here as well.

Pursuant to committee rules, all witnesses are to be sworn before they testify. If you could please rise and raise your right hand. We also get to get your picture. Do you solemnly swear or affirm that the testimony you're about to give will be the truth, the whole truth, and nothing but the truth so help you God?

Thank you. Let the record reflect that all witnesses answered in the affirmative.

In order to allow time for discussion, we would appreciate it if you would limit your verbal testimony to 5 minutes. Your entire written record and the attachments will be made part of the official record.

But Ms. Del Greco, let's start with you, and you are now recognized for 5 minutes.

Can I tell you all: these microphones in this committee, you've got to straighten them out, bring them right up uncomfortably close, and then there we go.

Ms. Del Greco, you're now recognized for 5 minutes.

WITNESS STATEMENTS

STATEMENT OF KIMBERLY DEL GRECO

Ms. DEL GRECO. Thank you, Chairman Chaffetz and Ranking Member Cummings and the members of the committee for this opportunity, along with our colleagues from NIST, with whom we have worked closely on a number of efforts.

I have submitted a written statement for record and will not take the committee's time to repeat all of the report. The statement provides a good description of the authorized programs we have in place. These programs utilize face technology to provide law enforcement partners with the needed capabilities to safeguard the American people.

It is crucial that authorized members of the law enforcement and national security communities have access to advanced biometric technologies to investigate, identify, apprehend, and prosecute terrorists and criminals.

The services and performance improvements in speed and accuracy delivered by the FBI's Next Generation Identification system, which includes face recognition technology, have enhanced our ability to solve crimes across the country.

With that said, the FBI's core value is strict adherence to the U.S. Constitution. The protection of the privacy and civil liberties of all persons in this country remains integral to the development and implementation of any new technology. The FBI's use of face recognition technology is confined within the same statutory, regulatory, and policy framework as all investigative initiatives by the FBI.

Today, I will discuss the following FBI programs which use face recognition technology for law enforcement purposes. They are, one, the FBI's Next Generation Identification Interstate Photo System; and two, the FACE Services Unit, both located at the FBI Criminal Justice Information Services Division.

Specifically, the Next Generation Identification Interstate Photo System allows for the searching of criminal mugshots authorized by law enforcement agencies. It is a search of law enforcement photos by law enforcement agencies for law enforcement purposes.

Law enforcement has performed photo lineups and manually reviewed mugshots for decades. Face recognition software allows this to be accomplished in an automated manner. Automated face recognition is an effective means of locating potential candidates for further investigation, but it remains an investigative lead only, and the candidates must be further reviewed by specialized face examiners and/or the relevant investigators.

The FBI has promulgated policies and procedures to emphasize that photos returned from the Next Generation Identification Interstate Photo System are not to be considered positive identifications and that the searches of the mugshots merely result in a ranked listing of candidates that require further investigation to determine a subject's true identity.

This guidance has been provided in the Next Generation Identification Interstate Photo System Policy and Implementation Guide,

which has been made available to authorized law enforcement users who receive candidate photos from the Next Generation Identification Interstate Photo System.

FACE Services: The FACE Services Unit provides investigative lead support to the FBI field offices, operational divisions, and legal attaches by comparing the face images of persons associated with an open FBI assessment or an active investigation against face images available in State and Federal photo repositories.

The FACE Services Unit only accepts probe photos that have been collected pursuant to appropriate legal authorities as part of an authorized FBI investigation. Upon receipt of the photo, the FACE Services Unit searches the photo using face recognition software against the database authorized for use by the FBI, which results in a photo gallery of potential candidates.

The FACE Services Unit performs comparisons of candidate photos against the probe photo to determine the candidate's value as an investigative lead. If a most likely candidate is found, it will be provided to the requesting FBI personnel; however, the FBI does not retain any photos that are not a most likely candidate.

As with the Next Generation Identification Interstate Photo System, this service does not provide a positive identification but rather an investigative lead and analysis to support that lead.

Finally, the FBI's strength is directly attributed to the dedication of its people who work for and on behalf of their fellow citizens. Our adversaries and the threats we face are relentless. The FBI must continue to identify and use new capabilities, such as an automated facial recognition system, to meet the high expectations for the FBI to preserve our Nation's freedom.

I want to thank my colleagues for their support and each and every FBI employee for their dedicated service. Thank you.

[Prepared statement of Ms. Del Greco follows:]

Statement of
Kimberly J. Del Greco
Deputy Assistant Director
Criminal Justice Information Services Division
Federal Bureau of Investigation

Before the
Committee on Oversight and Government Reform
U.S. House of Representatives

For a Hearing Concerning
Law Enforcement's Use of Facial Recognition Technology

March 22, 2017

Good afternoon Chairman Chaffetz, Ranking Member Cummings, and members of the committee. Thank you for the opportunity to appear before you today to discuss the Federal Bureau of Investigation's ("FBI") use of face recognition ("FR") technology.

FBI Programs Perform Face Recognition

The following FBI programs use FR technology for law enforcement purposes.[1] They are: (1) the FBI's Next Generation Identification ("NGI") System located at the FBI's Criminal Justice Information Services ("CJIS") Division, and (2) the Facial Analysis, Comparison, and Evaluation ("FACE") Services Unit also located at the FBI CJIS Division.

1. **NGI maintains a mugshot repository that is known as the Interstate Photo System ("IPS").** All mugshots are associated with tenprint fingerprints and a criminal history record. The NGI-IPS allows automated FR searches by authorized local, State, tribal, and Federal law enforcement agencies. The law enforcement agency submits a "probe" photo that is obtained pursuant to an authorized law enforcement investigation, to be searched against the mugshot repository. The NGI-IPS returns a gallery of "candidate" photos of 2-50 individuals (default is 20). The law enforcement agencies then must

[1]The Forensic Audio, Video and Image Analysis Unit ("FAVIAU") conducts Facial Identification examinations or "one to one" (1:1) image comparisons as a component of the forensic services in the Digital Evidence Laboratory. The FAVIAU works with the Office of the General Counsel for legal review of each case submitted in accordance with the Case Acceptance Policy. The Operational Technology Division and FAVIAU personnel have monitored the development of automated FR capabilities for two decades and have determined that the limitations of the technology do not make it suitable for use in forensic 1:1 casework, at this time.

manually review the candidate photos and perform further investigation to determine if any of the candidate photos are the same person as the probe photo.

The NGI-IPS technology is only used as an investigative lead, and not as a means of positive identification. The NGI-IPS *Policy Implementation Guide* has been made available to authorized law enforcement users who receive candidate photos from the Next Generation Identification-Interstate Photo System. The policy advises that the photos are not being provided as positive identification and cannot serve as the sole basis for law enforcement action. In addition, the FBI has promulgated policies and procedures that place legal, policy, and security requirements on the law enforcement users of the NGI-IPS, including a prohibition against submitting probe photos that were obtained in violation of the First or Fourth Amendments. It is important to note that the FBI does not retain the probe photos; the probes are searched and deleted. Therefore, the NGI-IPS remains a repository solely of mugshots that are submitted voluntarily with fingerprints pursuant to arrest.

2. **The FACE Services Unit** provides investigative lead support to the FBI Field Offices, Operational Divisions, and Legal Attaches by comparing the face images of persons associated with open assessments[2] and active investigations[3] against face images available in State and Federal FR systems. In limited instances, the FACE Services Unit provides FR support for closed FBI cases (*e.g.*, missing and wanted persons) and may offer recognition support to Federal partners. The FACE Services Unit only accepts "probe" photos that have been collected pursuant to applicable legal authorities as part of an authorized FBI investigation. Upon receipt of the photo(s), the FACE Services Unit searches them using FR software against databases authorized for use by the FBI, which results in a photo gallery of potential candidates. The FACE Services Unit performs manual comparisons of candidate photos against the probe photo(s) to determine a candidate's value as an investigative lead. This service does NOT provide positive identification, but rather, an investigative lead and analysis to support that lead.

---

[2]Per the Domestic Investigations and Operations Guide ("DIOG"), Section 5.4.1 Assessment Types and Section 5.5 Standards for Opening or Approving an Assessment, updated 09/28/2016 - Assessments may be opened to detect, obtain information about, or prevent or protect against Federal crimes or threats to the national security. They must have an authorized purpose and clearly defined objectives; they cannot be arbitrary or based on speculation. The Assessments must not be based solely on the exercise of First Amendment rights or on the race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity of the subject, or a combination of only such factors. The Assessment must be an appropriate use of personnel and financial resources.

[3]Per the DIOG, Section 6 Preliminary Investigations - Preliminary Investigations may be opened on the basis of "allegation or information" indicative of possible criminal activity or threats to national security. Full investigations may be opened when there is "an articulable factual basis" of possible criminal or national threat activity.

> In performing the search(es), the FACE Services Unit operates under the authority of the United States Code (U.S.C) Sections 533 and 534; Title 28, Code of Federal Regulations Section 0.85; Title 42, U.S.C. Section 3771; and Title 18, U.S.C. Chapter 123. The FACE Services Unit performs FR searches of FBI databases (*e.g.*, FBI's NGI), other Federal databases (*e.g.*, Department of State's Visa Photo File, Department of Defense's Automated Biometric Identification System, Department of State's Passport Photo File), and State photo repositories (*e.g.*, select State Departments of Motor Vehicles). Memoranda of Understanding and agreements have been established with all partners.

Privacy Impact Assessments ("PIAs") for the FACE Services Unit and the NGI-IPS have been prepared by the FBI, approved by the DOJ, and posted at https://www.fbi.gov/foia/privacy-impact-assessments. These PIAs provide to the public an accurate and complete explanation of how specific FBI components are using face recognition technology in support of the FBI's mission to defend against terrorism and enforce criminal laws, while protecting civil liberties. The PIAs also reflect many of the privacy and civil liberties choices made during the implementation of these programs.

Automated Face Recognition[4]

In addition to understanding how these FBI programs operate, it is also important to have an understanding of how automated FR works. The following is a brief description of automated FR: The automated FR software uses pattern matching approaches developed within the field of computer vision. Such approaches do not rely upon intrinsic models of what a face is, how it should appear, or what it may represent. In other words, the potential matching is not based on biological or anatomical models of what a face – or the features which make up a face – look like. Instead, the algorithm performance is entirely dependent upon the patterns which the algorithm developer finds to be most useful for matching. The patterns used in automated FR algorithms do not correlate to obvious anatomical features such as the eyes, nose or mouth in a one-to-one manner, although they are affected by these features. Put another way, the algorithms "see" faces in a way that differs from how humans see faces.

Accuracy

The FBI conducted a trade study of FR products, leveraging the NGI Integrator Lockheed Martin, which led to the determination of MorphoTrust as the best cost solution in Fall 2010. The FBI has tested and verified that the NGI FR Solution returns the correct candidate a minimum of 85 percent of the time within the top 50 candidates.

---

[4]In addition to the use of automated FR technology to search probe images against a gallery, as described for the NGI, the FBI also utilizes automated FR as a way to organize or "triage" digital image files which have been obtained pursuant to an authorized law enforcement investigation.

The FBI manages the CJIS Division, Advisory Policy Board ("APB") Process, which holds meetings twice a year. The APB is comprised of members of local, State, tribal, and Federal criminal justice agencies that contribute to and use CJIS systems and information. It is responsible for reviewing policy issues and appropriate technical and operational issues related to FBI CJIS programs (such as the NGI) administered by the FBI's CJIS Division, and thereafter, making appropriate recommendations. Through the APB Process, users can provide feedback and suggestions or bring issues to the attention of the FBI's CJIS Division. To date, no users have submitted concerns to the FBI regarding the accuracy of face searches conducted on the NGI-IPS.

Audits

The FBI performs audits as they serve an important role in identifying and mitigating risks associated with users of information systems not meeting policy requirements. In a recent Audit of the FBI's use of FR by the Government Accountability Office ("GAO"), the FBI advised that the NGI-IPS operated in a limited capacity as a pilot program from December 2011 through April 2015. While the early stages of planning for formal NGI-IPS audits began during the system's pilot phase and prior to GAO's review, the formal draft audit plan was completed on schedule in summer 2015 and approved by the CJIS APB in June 2016.

The FBI worked with the APB and agreed upon an audit schedule that includes use of the NGI-IPS, although the number of actual NGI-IPS participants is currently limited. The FBI CJIS Division's CJIS Audit Unit ("CAU") currently executes the formal audits to assess compliance with requirements primarily derived from the *NGI-IPS Policy and Implementation Guide*. The audit is conducted in conjunction with existing National Identity Services Audits externally at State Identification Bureaus and Federal agencies, and may include reviews at a selection of local agencies that access the NGI-IPS. The NGI-IPS audit plan also provides for an internal audit of the FACE Services Unit to be conducted in accordance with existing procedures for FBI internal audits associated with CJIS system access. Procedures for both external and internal audits include review of NGI-IPS system transaction records and associated supporting documentation provided by audit participants.

Currently eleven States have connectivity with the NGI-IPS and as of February 2017, the FBI has conducted NGI-IPS audits at the following four States:

- Maine – 06/16/2016
- Michigan – 06/16/2016
- Delaware – 10/16/2016
- Arizona – 02/17/2017

No significant findings of noncompliance have been identified during the four NGI-IPS audits and there have been no observations of unauthorized requests or misuse of the NGI-IPS. However, three relatively minor issues were identified at one State:

- Enrollment Discrepancy: The State submitted 1.3 million criminal photos to the CJIS Division in bulk. Of the 1.3 million submissions, 450,000 were rejected back to the State because the Date of Arrest ("DOA") did not match the DOA on file with the FBI.
- Area of Concern: The State did not have an established NGI-IPS training program.
- Area of Concern: The State did not have written procedures for the proper enrollment of Scars, Marks, and Tattoos.

***It should be noted that these issues are tentative, pending finalization of the audit results.*

Additionally, the CAU has scheduled the audit of the FACE Services Unit for 2018 to coincide with the existing triennial FBI internal audit.

Closing

Finally, the FBI's strength is directly attributed to the dedication of its people who work for and on behalf of their fellow citizens. Our adversaries and the threats we face are relentless. The FBI must continue to identify and use new capabilities such as automated FR to meet the high expectations for the FBI to preserve our nation's freedoms, ensure our liberties are protected, and preserve our security. Quite simply put, we at the FBI cannot fail to meet our assigned mission. We must continue to exceed expectations and never rest on past successes. Hence, we must embrace new technologies such as automated FR and optimize allocated resources to achieve mission objectives. I want to thank all of my colleagues for their support, and each and every employee at the FBI for their dedicated services. I am pleased to answer any questions you might have.

Chairman CHAFFETZ. Thank you.

Director, you're now recognized for 5 minutes.

STATEMENT OF DIANA MAURER

Ms. MAURER. Good morning, Mr. Chairman, Ranking Member Cummings, and other members and staff. I'm pleased to be here today to discuss the findings from our review of the FBI's use of facial recognition.

We're all familiar with the general idea behind this technology, and it's a good one: Instead of relying on books of mugshots from the "Hill Street Blues" era, law enforcement can use "CSI"-era computers to nearly instantly identify a criminal from a grainy crime scene photo. Of course, that's the idea. The reality is far from what we currently see in movies or TV.

Face recognition is relatively new for the FBI, and there are significant technical and legal limitations on what it can do. Even so, it's a valuable tool that can greatly enhance the efficiency and effectiveness of Federal law enforcement.

The FBI uses face recognition in two ways: First, it developed a system that currently has over 50 million images for State, local, and FBI use; second, the FBI accesses other systems at the Departments of Defense and State as well as driver's license photos from 18 States, with total potential access to over 400 million images.

Used properly, face recognition can help make us all safer. However, the pictures of millions of Americans, including millions with no criminal convictions, are being searched by the FBI, which is why attention to privacy and accuracy is so important. We found that the FBI needs to do a better job on both fronts.

First, we'll talk about privacy. Federal law requires agencies to publicly share how they plan to use personal information, such as facial images, when they roll out a new capability and when they update it. We found that the Department of Justice and the FBI did not do so in a timely manner.

Specifically, DOJ initially published a Privacy Impact Assessment for the Interstate Photo System in 2008; however, the FBI did not update or publish a new assessment before it began using the system or made significant changes to it. DOJ also did not approve a privacy assessment when the FBI began accessing other systems to support its own investigations.

The FBI eventually issued privacy assessments in 2015 during our review and over 3 years after they began using both systems. During that time, the public remained unaware of how facial images were being used because the assessments were not published as required.

We also had several concerns about the FBI's efforts to ensure accuracy. There are two key aspects to accuracy for facial recognition: the detection rate, how often it correctly generates a match; and the false positive rate, how often it incorrectly generates a match. We have concerns about how the FBI approaches both measures.

In tests, the FBI system generated a correct match 86 percent of the time, 1 percent more than the requirement. How the FBI defined a match is important. For each query, the system generated 50 potential images. If the correct image was among the 50, it was

scored as a match. In the real world, however, users frequently only generate the top handful of images, which requires a much higher degree of accuracy for the results to be useful to investigators.

Further, the FBI does not test for false positives. So it doesn't know how often a system incorrectly identifies someone as the potential suspect. High levels of false positives could hinder criminal investigations with false leads. Further, innocent people could bear the burden of being falsely accused, including the implications of Federal investigators showing up at their home or place of business.

Finally, the FBI has not assessed the accuracy of face recognition systems operated by external partners to ensure they are sufficiently accurate to support FBI investigations. We made six commonsense recommendations to help address these problems, but we were, frankly, concerned when the Department and the FBI only fully agreed with one.

The good news is that the FBI has begun taking steps to address two of our recommendations. My hope is that, in the aftermath of today's hearing, the FBI and the Department will decide to take action to fully address all six.

Face recognition could prove to be an immensely valuable tool in solving crime and enhancing national security, but the FBI and DOJ need to take further action to address privacy and accuracy concerns. Doing so will help inform the public on how facial images are being used, enhance the efficiency of law enforcement, and avoid wasting valuable investigative resources, and unnecessarily involving innocent people.

Mr. Chairman, thank you for the opportunity to testify today. I look forward to your questions.

[Prepared statement of Ms. Maurer follows:]

United States Government Accountability Office

GAO

Testimony

Before the Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 9 a.m. ET
Wednesday, March 22, 2017

FACE RECOGNITION TECHNOLOGY

DOJ and FBI Need to Take Additional Actions to Ensure Privacy and Accuracy

Statement of Diana Maurer, Director,
Homeland Security and Justice

GAO Highlights

Highlights of GAO-17-489T, a testimony before the Committee on Oversight and Government Reform, House of Representatives

March 2017

FACE RECOGNITION TECHNOLOGY

DOJ and FBI Need to Take Additional Actions to Ensure Privacy and Accuracy

Why GAO Did This Study

Technology advancements have increased the overall accuracy of automated face recognition over the past few decades. This technology has helped law enforcement agencies identify criminals in their investigations. However, privacy advocates and members of the Congress remain concerned regarding the accuracy of the technology and the protection of privacy and individual civil liberties when technologies are used to identify people based on their biological and behavioral characteristics.

This statement describes the extent to which the FBI ensures adherence to laws and policies related to privacy regarding its use of face recognition technology, and ensure its face recognition capabilities are sufficiently accurate. This statement is based on our in May 2016 report regarding the FBI's use of face recognition technology and includes agency updates to our recommendations. To conduct that work, GAO reviewed federal privacy laws, FBI policies, operating manuals, and other documentation on its face recognition capability. GAO interviewed officials from the FBI and the Departments of Defense and State, which coordinate with the FBI on face recognition. GAO also interviewed two state agencies that partner with FBI to use multiple face recognition capabilities.

What GAO Recommends

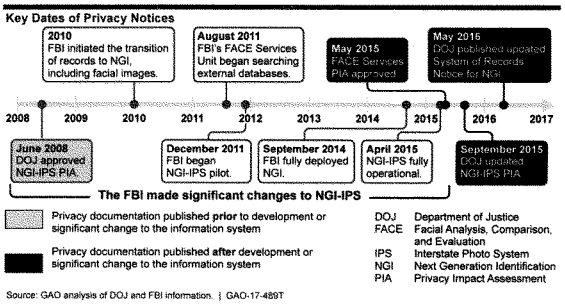
In May 2016, DOJ and the FBI partially agreed with two recommendations and disagreed with another on privacy. FBI agreed with one and disagreed with two recommendations on accuracy. GAO continues to believe that the recommendations are valid.

View GAO-17-489T. For more information, contact Diana Maurer at (202) 512-8777or maurerd@gao.gov.

What GAO Found

In May 2016, GAO found that the Federal Bureau of Investigation (FBI) had not fully adhered to privacy laws and policies and had not taken sufficient action to help ensure accuracy of its face recognition technology. GAO made six recommendations to address these issues. As of March 2017, the Department of Justice (DOJ) and the FBI disagreed with three recommendations and had taken some actions to address the remainder, but had not fully implemented them.

Privacy notices not timely. In May 2016, GAO recommended DOJ determine why privacy impact assessments (PIA) were not published in a timely manner (as required by law) and take corrective action. GAO made this recommendation because FBI did not update the Next Generation Identification-Interstate Photo System (NGI-IPS) PIA in a timely manner when the system underwent significant changes or publish a PIA for Facial Analysis, Comparison and Evaluation (FACE) Services before that unit began supporting FBI agents. DOJ disagreed on assessing the PIA process stating it established practices that protect privacy and civil liberties beyond the requirements of the law. GAO also recommended DOJ publish a system of records notice (SORN) and assess that process. DOJ agreed to publish a SORN, but did not agree there was a legal requirement to do so. GAO believes both recommendations are valid to keep the public informed on how personal information is being used and protected by DOJ components.



Source: GAO analysis of DOJ and FBI information. | GAO-17-489T

GAO also recommended the FBI conduct audits to determine if users of NGI-IPS and biometric images specialists in the FBI's FACE unit are conducting face image searches in accordance with DOJ policy requirements. The FBI began conducting NGI-IPS user audits in 2017.

Accuracy testing limited. In May 2016, GAO recommended the FBI conduct tests to verify that NGI-IPS is accurate for all allowable candidate list sizes to give more reasonable assurance that NGI-IPS provides leads that help enhance criminal investigations. GAO made this recommendation because FBI officials stated that they do not know, and have not tested, the detection rate for candidate list sizes smaller than 50, which users sometimes request from the

FBI. GAO also recommended the FBI take steps to determine whether systems used by external partners are sufficiently accurate for FBI's use. By taking such steps, the FBI could better ensure the data from external partners do not unnecessarily include photos of innocent people as investigative leads. However, FBI disagreed with these two recommendations, stating the testing results satisfy requirements for providing investigative leads and that FBI does not have authority to set accuracy requirements for external systems. GAO continues to believe these recommendations are valid because the recommended testing and determination of accuracy of external systems would give the FBI more reasonable assurance that the systems provide investigative leads that help enhance, rather than hinder or overly burden, criminal investigation work.

GAO also recommended the FBI conduct an annual operational review of NGI-IPS to determine if the accuracy of face recognition searches is meeting federal, state, and local law enforcement needs and take actions, as necessary. DOJ agreed and in 2017 FBI stated they implemented the recommendation by submitting a paper to solicit feedback from NGI-IPS users on whether face recognition searches are meeting their needs. However, GAO believes these actions do not fully meet the recommendation because they did not result in any formal response from users and did not constitute an operational review. GAO continues to recommend FBI conduct an operational review of NGI-IPS at least annually.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee:

I am pleased to be here today to discuss our work on the Federal Bureau of Investigation's (FBI) use of face recognition technology. As the law enforcement community adopts face recognition technology for investigative purposes, academics, privacy advocates, and members of the Congress have questioned whether it is sufficiently accurate for this use. In addition, the use of face recognition technology raises questions regarding the protection of privacy and individual civil liberties. Face recognition technology mimics how people identify others: by scrutinizing their face. However, what is an effortless skill in humans has proven difficult to replicate in machines, although computer and technology advancements over the past few decades have increased the overall accuracy of automated face recognition. According to officials from the FBI, these advancements in face recognition technology can help law enforcement agencies identify criminals in federal, state and local investigations. For example, the FBI and one of its state partners used face recognition in June 2015 to help identify a sex offender who had been a fugitive for nearly 20 years.

This statement describes the extent to which the FBI (1) ensures adherence to laws and policies related to privacy regarding its use of face recognition technology, and (2) ensures its face recognition capabilities are sufficiently accurate. This statement is based on our prior work issued in May 2016 regarding the FBI's use of face recognition technology and includes additional agency response to our recommendations.[1] The work upon which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. More information on our scope and methodology can be found in our May 2016 report.[2]

[1]GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, GAO-16-267 (Washington, D.C.: May 16, 2016).

[2]GAO-16-267.

Background

FBI's Use of Face Recognition Technology

For decades, fingerprint analysis has been the most widely used biometric technology for positively identifying arrestees and linking them with any previous criminal record. Beginning in 2010, the FBI began incrementally replacing the Integrated Automated Fingerprint Identification System (IAFIS) with Next Generation Identification (NGI) at an estimated cost of $1.2 billion.[3] NGI was not only to include fingerprint data from IAFIS and biographic data, but also to provide new functionality and improve existing capabilities by incorporating advancements in biometrics, such as face recognition technology. As part of the fourth of six NGI increments, the FBI updated the Interstate Photo System (IPS) to provide a face recognition service that allows law enforcement agencies to search a database of about 30 million photos to support criminal investigations.[4]

NGI-IPS users include the FBI and selected state and local law enforcement agencies, which can submit search requests to help identify an unknown person using, for example, a photo from a surveillance camera.[5] When a state or local agency submits such a photo, NGI-IPS uses an automated process to return a list of 2 to 50 possible candidate photos from the database, depending on the user's specification.[6] Figure 1 describes the process for a search requested by state or local law enforcement.

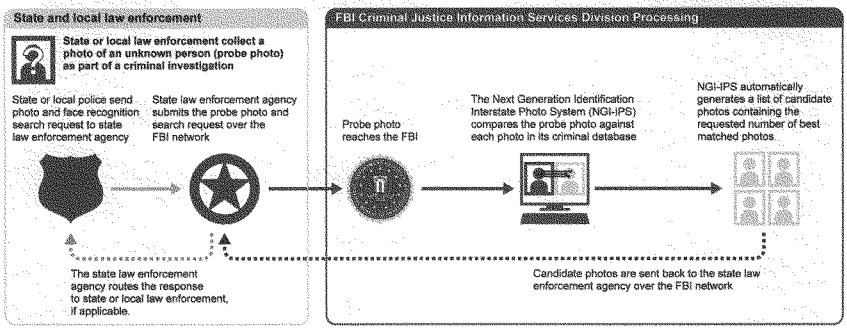
[3]IAFIS was a national, computerized system for storing, comparing, and exchanging fingerprint data in a digital format. The FBI expects to complete the last NGI increment by 2017.

[4]The 30 million photos in NGI-IPS represent about 16.9 million individuals and reflect figures as of December 2015. When the FBI implemented IAFIS in 1999, the Criminal Justice Information Services (CJIS) Division began storing mugshots submitted with fingerprints in a photo database and also digitized all previously submitted hardcopy mugshots. However, until the implementation of NGI, users could only search for photos using the person's name or unique FBI number.

[5]The FBI began a pilot of NGI-IPS in December 2011, and NGI-IPS became fully operational in April 2015.

[6]We reported in May 2016 that as of December 2015, the FBI had agreements with 7 states to search NGI-IPS, and was working with more states to grant access. At the time of our review, FBI officials stated that the FBI did not offer this service to other federal agencies.

Figure 1: Description of the Federal Bureau of Investigation's (FBI) Face Recognition System Request and Response Process for State and Local Law Enforcement



Source: GAO analysis of FBI documentation. | GAO-17-489T

In addition to the NGI-IPS, the FBI has an internal unit called Facial Analysis, Comparison and Evaluation (FACE) Services that provides face recognition capabilities, among other things, to support active FBI investigations.[7] FACE Services not only has access to NGI-IPS, but can search or request to search databases owned by the Departments of State and Defense and 16 states, which use their own face recognition systems.[8] Figure 2 shows which states partnered with FBI for FACE Services requests, as of August 2016. Unlike NGI-IPS, which primarily contains criminal photos, these external systems primarily contain civil photos from state and federal government databases, such as driver's license photos and visa applicant photos. The total number of face photos available in all searchable repositories for FACE Services is over 411

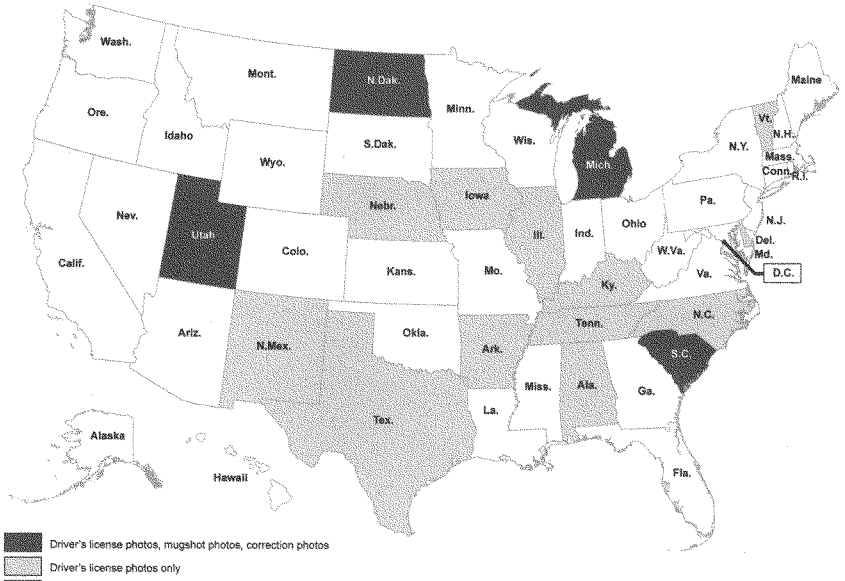
[7]FACE Services began supporting investigations in August 2011.

[8]According to FBI officials, the external photo databases do not contain privately obtained photos or photos from social media, and the FBI does not maintain these photos. Also, according to FBI officials, legal authority exists for the face recognition searching of all of these photo databases. For example, FBI officials stated that the states are authorized to use the law enforcement exception of the Driver's Privacy Protection Act to permit sharing photos with the FBI. Further, the FBI also has memorandums of understanding (MOUs) with their partner agencies that describe the legal authorities that allow the FBI to search the partner agencies' photos.

million, and the FBI is interested in adding additional federal and state face recognition systems to its search capabilities.[9] Biometric images specialists for FACE Services manually review candidate photos from their external partners before returning at most the top 1 or 2 photos as investigative leads to the requesting FBI agents. However, according to FACE Services officials, if biometric images specialists determine that none of the databases returned a likely match, they do not return any photos to the agents.

[9]The over 411 million refers to photos, not identities and reflects data as of December 2015.

Figure 2: Information Available for the Federal Bureau of Investigation (FBI) Facial Analysis, Comparison, and Evaluation (FACE) Services' Photo Searches, by State



Source: GAO analysis of FBI information; Map Resources (map). | GAO-17-489T

[a]Some state laws prohibit face recognition.

Privacy Laws

Federal agency collection and use of personal information, including face images, is governed primarily by two laws: the Privacy Act of 1974[10] and the privacy provisions of the E-Government Act of 2002.[11]

- The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public through a system of records notice (SORN) in the Federal Register.[12] According to the Office of Management and Budget (OMB) guidance, the purposes of the notice are to inform the public of the existence of systems of records; the kinds of information maintained; the kinds of individuals on whom information is maintained; the purposes for which they are used; and how individuals can exercise their rights under the Privacy Act.[13]
- The E-Government Act of 2002 requires that agencies conduct Privacy Impact Assessments (PIAs) before developing or procuring information technology (or initiating a new collection of information) that collects, maintains, or disseminates personal information. The assessment helps agencies examine the risks and effects on individual privacy and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. OMB guidance also requires agencies to perform and update PIAs as necessary where a system change creates new privacy risks, for example, when the adoption or alteration of business processes results in personal information in government databases being merged, centralized, matched with other databases or otherwise significantly manipulated.[14]

[10]Pub. L. No. 93-579 (Dec. 31, 1974), as amended; 5 U.S.C. 552a.

[11]Sec. 208(b), Pub. L. No. 107-347 (Dec. 17, 2002); 44 U.S.C. 3501 note.

[12]A system of record is defined by the Privacy Act of 1974 as a group of records containing personal information under the control of any agency from which information is retrieved by the name of an individual or by an individual identifier.; 5 U.S.C. 552a(a)(4)&(5).

[13]OMB, Privacy Act Implementation: Guidelines and Responsibilities, 40 FR 28948, 28962 (July 9, 1975).

[14]M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003).

DOJ and FBI Did Not Provide Timely Transparency and Have Not Fully Implemented Recommendations to Protect Privacy

DOJ Has an Oversight Structure in Place to Protect Privacy, but Did Not Publish Required Notices in a Timely Manner

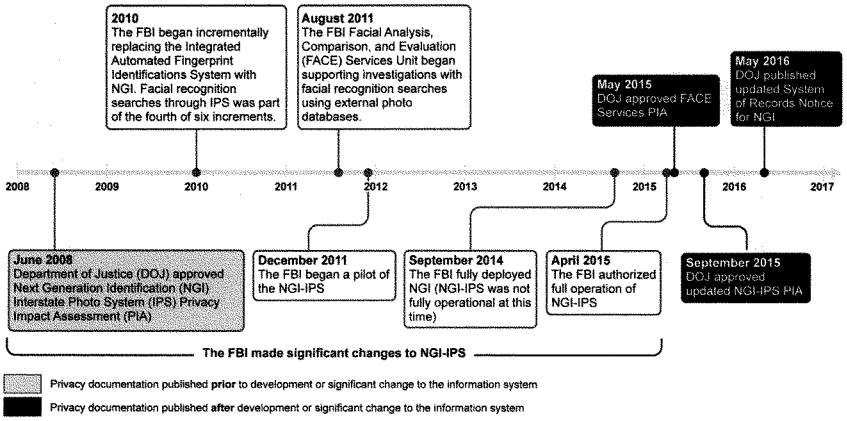
Within the Department of Justice (DOJ), preserving civil liberties and protecting privacy is a responsibility shared by department level offices and components. As such, DOJ and the FBI have established oversight structures to help protect privacy and oversee compliance with statutory requirements. For example, while the FBI drafts privacy documentation for its face recognition capabilities, DOJ offices review and approve key documents developed by the FBI—such as PIAs and SORNs. However, the FBI did not update the NGI-IPS PIA in a timely manner when the system underwent significant changes and did not develop and publish a PIA for FACE Services before that unit began supporting FBI agents. Additionally, DOJ did not publish a SORN that addresses the collection and maintenance of photos accessed and used through the FBI's face recognition capabilities until after our 2016 review.

Consistent with the E-Government Act and OMB guidance, DOJ developed guidance that requires initial PIAs to be completed at the beginning of development of information systems and any time there is a significant change to the information system in order to determine whether there are any resulting privacy issues. DOJ published a PIA at the beginning of the development of NGI-IPS in 2008, as required.[15] However, the FBI did not publish a new PIA or update the 2008 PIA before beginning to pilot NGI-IPS in December 2011 or as significant

[15]Specifically, in 2008 the FBI published a PIA of its plans for NGI-IPS and indicated it was in the study phase, which included development of functional and system requirements.

changes were made to the system through September 2015.[16] During that time, the FBI used NGI-IPS to conduct over 20,000 searches to assist in investigations throughout the pilot. Similarly, DOJ did not approve a PIA for FACE Services when it began supporting investigations in August 2011. As a new use of information technology involving the handling of personal information, it too, required a PIA.[17] Figure 3 provides key dates in the implementation of these face recognition capabilities and the associated privacy notices.

Figure 3: Key Dates in the Implementation of the Federal Bureau of Investigation's (FBI) Face Recognition Capabilities and Associated Privacy Impact Assessments and System of Records Notice



Source: GAO analysis of DOJ and FBI information. | GAO-17-489T

[16]In December 2011, as part of a pilot program, the FBI began incrementally allowing a limited number of states to submit face recognition searches against a subset of criminal images in the FBI's database. Beginning in April 2015, states started transitioning from the pilot to full operational capability.

[17]The FBI conducted a privacy threshold assessment of FACE Services in 2012 that determined a PIA was necessary for the work log used to store personal information.

During the course of our review, DOJ approved the NGI-IPS PIA in September 2015 and the FACE Services PIA in May 2015—over three years after the NGI-IPS pilot began and FACE Services began supporting FBI agents with face recognition services. DOJ and FBI officials stated that these PIAs reflect the current operation of NGI-IPS and FACE Services. However, as the internal drafts of these PIAs were updated, the public remained unaware of the department's consideration for privacy throughout development of NGI-IPS and FACE Services. This is because the updates were not published, as required.[18] Specifically, delays in the development and publishing of up-to-date PIAs for NGI-IPS and FACE Services limited the public's knowledge of how the FBI uses personal information in the face recognition search process.

Additionally, DOJ did not publish a SORN, as required by the Privacy Act, that addresses the collection and maintenance of photos accessed and used through the FBI's face recognition capabilities until May 5, 2016—after completion of our review. At that time, the FBI published a new SORN that reported the modification of the Fingerprint Identification Records System to be renamed the Next Generation Identification (NGI) System.[19] However, according to OMB guidance then in effect, the SORN must appear in the Federal Register before the agency begins to operate the system, e.g., collect and use the information.[20] While the new SORN addresses face recognition, those capabilities have been in place since 2011. Throughout this period, the agency collected and maintained personal information for these capabilities without the required explanation of what information it is collecting or how it is used. Completing and publishing SORNs in a timely manner is critical to providing transparency to the public about the personal information agencies plan to collect and how they plan to use the information.

[18]FBI officials stated that they drafted an updated PIA for NGI-IPS in January 2015 and submitted it to DOJ for review—before NGI-IPS became fully operational in April 2015.

[19]According to DOJ officials, the FBI initially waited to complete the NGI SORN until all of NGI's capabilities were identified in order to provide a comprehensive explanation of NGI and limit the number of necessary SORN revisions.

[20]OMB Circular A-130, App. I, sec. 5.a(2)(a) (2000).

DOJ Disagrees with GAO's Recommendations regarding Privacy

In our May 2016 report, we made two recommendations to DOJ regarding its processes to develop privacy documentation, and DOJ officials disagreed with both. We recommended that DOJ assess the PIA development process to determine why PIAs were not published prior to using or updating face recognition capabilities. DOJ officials did not concur with this recommendation, and stated that the FBI has established practices that protect privacy and civil liberties beyond the requirements of the law. Further, DOJ stated that it developed PIAs for both FACE Services and NGI-IPS, as well as other privacy documentation, throughout the development of the these capabilities that reflect privacy choices made during their implementation. For example, DOJ officials stated that it revised the FACE Services PIA as decisions were made. We agree that, during the course of our review, DOJ published PIAs for both FACE Services and NGI-IPS. However, as noted in the report, according to the E-Government Act and OMB and DOJ guidance, PIAs are to be assessments performed before developing or procuring technologies and upon significant system changes. Further, DOJ guidance states that PIAs give the public notice of the department's consideration of privacy from the beginning stages of a system's development throughout the system's life cycle and ensures that privacy protections are built into the system from the start–not after the fact–when they can be far more costly or could affect the viability of the project. In its response to our draft report, DOJ officials stated that it will internally evaluate the PIA process as part of the Department's overall commitment to improving its processes, not in response to our recommendation.

In March 2017, we followed up with DOJ to obtain its current position on our recommendation. DOJ continues to believe that its approach in designing the NGI system was sufficient to meet legal privacy requirements and that our recommendation represents a "checkbox approach" to privacy. We disagree with DOJ's characterization of our recommendation. We continue to believe that the timely development and publishing of future PIAs would increase transparency of the department's systems. We recognize the steps the agency took to consider privacy protection during the development of the NGI system. We also stand by our position that notifying the public of these actions is important and provides the public with greater assurance that DOJ components are evaluating risks to privacy when implementing systems.

We also recommended DOJ develop a process to determine why a SORN was not published for the FBI's face recognition capabilities prior to using NGI-IPS, and implement corrective actions to ensure SORNs are published before systems become operational. DOJ agreed, in part, with

our recommendation and submitted the SORN for publication after we provided our draft report for comment. However:

- DOJ did not agree that the publication of a SORN is required by law. We disagree with DOJ's interpretation regarding the legal requirements of a SORN. The Privacy Act of 1974 requires that when agencies establish or make changes to a system of records, they must notify the public through a SORN published in the Federal Register.[21] DOJ's comments on our draft report acknowledge that the automated nature of face recognition technology and the sheer number of photos now available for searching raise important privacy and civil liberties considerations.
- DOJ officials also stated that the FBI's face recognition capabilities do not represent new collection, use, or sharing of personal information. We disagree. We believe that the ability to perform automated searches of millions of photos is fundamentally different in nature and scope than manual review of individual photos, and the potential impact on privacy is equally fundamentally different. By assessing the SORN development process and taking corrective actions to ensure timely development of future SORNs, the public would have a better understanding of how personal information is being used and protected by DOJ components.

FBI Agreed to Conduct Audits to Oversee the Use of NGI-IPS and FACE Services

The Criminal Justice Information Services (CJIS), which operates FBI's face recognition capabilities, has an audit program to evaluate compliance with restrictions on access to CJIS systems and information by its users, such as the use of fingerprint records. However, at the time of our review, it had not completed audits of the use of NGI-IPS or FACE Services searches of external databases. State and local users have been accessing NGI-IPS since December 2011 and have generated IPS transaction records since then that would enable CJIS to assess user compliance.[22] In addition, the FACE Services Unit has used external databases that include primarily civil photos to support FBI investigations since August 2011, but the FBI had not audited its use of these

[21] 5 U.S.C. 552a(e)(4)(B).

[22] Transaction records are a log of communications between CJIS and CJIS system users. NGI-IPS transaction records would include, among other things, tenprint submissions transactions, images submissions for an existing identity, face recognition search requests, and face image search results.

databases.[23] *Standards for Internal Control in the Federal Government* call for federal agencies to design and implement control activities to enforce management's directives and to monitor the effectiveness of those controls.[24] In 2016, we recommended that the FBI conduct audits to determine the extent to which users of NGI-IPS and biometric images specialists in FACE Services are conducting face image searches in accordance with CJIS policy requirements.

DOJ partially concurred with our recommendation. Specifically, DOJ concurred with the portion of our recommendation related to the use of NGI-IPS. DOJ officials stated that the FBI specified policy requirements with which it could audit NGI-IPS users in late 2014, completed a draft audit plan during the course of our review in summer 2015, and expects to begin auditing use of NGI-IPS in fiscal year 2016. As of March 2017, DOJ reported that the CJIS Audit Unit began assessing NGI-IPS requirements at participating states in conjunction with its triennial National Identity Services audit and that as of February 2017, the unit had conducted NGI-IPS audits of four states.

At the time we issued our 2016 report, DOJ officials did not fully comment on the portion of our recommendation that the FBI audit the use of external databases, because FBI officials said the FBI does not have authority to audit these systems. As noted in the report, we understand the FBI may not have authority to audit the maintenance or operation of databases owned and managed by other agencies. However, the FBI does have a responsibility to oversee the use of the information by its own employees. As a result, our recommendation focuses on auditing both NGI-IPS users, such as states and FACE Services employees, as well as FACE Services employees' use of information received from external databases—not on auditing the external databases. We continue to believe that the FBI should audit biometric images specialists' use of information received from external databases to ensure compliance with FBI privacy policies and to ensure images are not disseminated for unauthorized purposes or to unauthorized recipients. In March 2017, DOJ provided us with the audit plan the CJIS Audit Unit developed in June 2016 for NGI-IPS users. DOJ officials said CJIS developed an audit plan

[23]Unlike NGI-IPS which primarily contains criminal photos, these external systems primarily contain civil photos from state and federal government databases, such as visa applicant photos and selected states' driver's license photos.

[24]9GAO, *Internal Control: Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: Nov. 1999).

of the FACE Services Unit to coincide with the existing triennial FBI internal audit for 2018. However, DOJ did not provide the audit plan for the FACE Services Unit. DOJ officials said the methodology would be the same as the audit plan for NGI-IPS, but that methodology does not describe oversight on use of information obtained from external systems accessed by FACE Services employees. Therefore, we believe DOJ is making progress towards meeting, but has not fully implemented our recommendation.

FBI Has Taken Limited Actions to Address Our Recommendations for Ensuring the Accuracy of its Face Recognition Capabilities

FBI Has Conducted Limited Assessments of the Accuracy of NGI-IPS Face Recognition Searches

In May 2016, we reported that prior to accepting and deploying NGI-IPS, the FBI conducted testing to evaluate how accurately face recognition searches returned matches to persons in the database. However, the tests were limited because they did not include all possible candidate list sizes and did not specify how often incorrect matches were returned.[25] According to the National Science and Technology Council and the National Institute of Standards and Technology, the detection rate (how often the technology generates a match when the person is in the database) and the false positive rate (how often the technology incorrectly generates a match to a person in the database) are both necessary to assess the accuracy of a face recognition system.[26] The FBI's detection

[25]NGI-IPS automatically generates a list of candidate photos containing the requested number of best matched photos.

[26]National Science and Technology Council, *Biometrics Frequently Asked Questions* (Sept. 7, 2006) and National Institute of Standards and Technology, *Face Recognition Vendor Test: NIST Interagency Report 8009* (May 26, 2014).

rate requirement for face recognition searches states when the person exists in the database, NGI-IPS shall return a match of this person at least 85 percent of the time (the detection rate). However, the FBI only tested this requirement with a candidate list of 50 potential matches. In these tests, according to FBI documentation, 86 percent of the time, a match to a person in the database was correctly returned. Further, FBI officials stated that they have not assessed how often NGI-IPS face recognition searches erroneously match a person to the database (the false positive rate). As a result, we recommended that the FBI conduct tests of NGI-IPS to verify that the system is sufficiently accurate for all allowable candidate list sizes and ensure that both the detection rate and the false positive rate are identified for such tests.

With the recommended testing, the FBI would have more reasonable assurance that NGI-IPS provides investigative leads that help enhance, rather than hinder or overly burden, criminal investigation work. If false positives are returned at a higher than acceptable rate, law enforcement users may waste time and resources pursuing unnecessary investigative leads. In addition, the FBI would help ensure that it is sufficiently protecting the privacy and civil liberties of U.S. citizens enrolled in the database. Specifically, according to a July 2012 Electronic Frontier Foundation hearing statement, false positives can alter the traditional presumption of innocence in criminal cases by placing more of a burden on the defendant to show he is not who the system identifies him to be. [27] The Electronic Frontier Foundation argues that this is true even if a face recognition system such as NGI-IPS provides several matches instead of one, because each of the potentially innocent individuals identified could be brought in for questioning.

In comments on our draft report in 2016, and reiterated during recommendation follow-up, as of March 2017, DOJ did not concur with this recommendation. DOJ officials stated that the FBI has performed accuracy testing to validate that the system meets the requirements for the detection rate, which fully satisfies requirements for the investigative lead service provided by NGI-IPS.

[27] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcommittee on Privacy, Technology and the Law of the Senate Committee on the Judiciary*, 112th Cong. 24 (2012) (statement of Jennifer Lynch, Staff Attorney, Electronic Frontier Foundation).

We disagree with DOJ. A key focus of our recommendation is the need to ensure that NGI-IPS is sufficiently accurate for all allowable candidate list sizes. Although the FBI has tested the detection rate for a candidate list of 50 photos, NGI-IPS users are able to request smaller candidate lists—specifically between 2 and 50 photos. FBI officials stated that they do not know, and have not tested, the detection rate for other candidate list sizes. According to these officials, a smaller candidate list would likely lower the detection rate because a smaller candidate list may not contain a likely match that would be present in a larger candidate list. However, according to the FBI Information Technology Life Cycle Management Directive, testing needs to confirm the system meets all user requirements. Because the accuracy of NGI-IPS's face recognition searches when returning fewer than 50 photos in a candidate list is unknown, the FBI is limited in understanding whether the results are accurate enough to meet NGI-IPS users' needs.

DOJ officials also stated that searches of NGI-IPS produce a gallery of likely candidates to be used as investigative leads, not for positive identification.[28] As a result, according to DOJ officials, NGI-IPS cannot produce false positives and there is no false positive rate for the system. We disagree with DOJ. The detection rate and the false positive rate are both necessary to assess the accuracy of a face recognition system. Generally, face recognition systems can be configured to allow for a greater or lesser number of matches. A greater number of matches would generally increase the detection rate, but would also increase the false positive rate. Similarly, a lesser number of matches would decrease the false positive rate, but would also decrease the detection rate. Reporting a detection rate of 86 percent without reporting the accompanying false positive rate presents an incomplete view of the system's accuracy.

[28]The term "positive identification" means a determination, based upon a comparison of fingerprints or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record.

FBI Agreed to Conduct Annual Operational Reviews of NGI-IPS

FBI, DOJ, and OMB guidance all require annual reviews of operational information technology systems to assess their ability to continue to meet cost and performance goals.[29] For example, the FBI's Information Technology Life Cycle Management Directive requires an annual operational review to ensure that the fielded system is continuing to support its intended mission, among other things. In 2016, we reported that the FBI had not assessed the accuracy of face recognition searches of NGI-IPS in its operational setting—the setting in which enrolled photos, rather than a test database of photos—are used to conduct a search for investigative leads. According to FBI officials, the database of photos used in its tests is representative of the photos in NGI-IPS, and ongoing testing in a simulated environment is adequate. However, according to the National Institute of Standards and Technology, as the size of a photo database increases, the accuracy of face recognition searches performed on that database can decrease due to lookalike faces.[30] FBI's test database contains 926,000 photos while NGI-IPS contains about 30 million photos. As a result, we recommended the FBI conduct an operational review of NGI-IPS at least annually that includes an assessment of the accuracy of face recognition searches to determine if it is meeting federal, state, and local law enforcement needs and take actions, as necessary, to improve the system.

In 2016, DOJ concurred with this recommendation. As of March 2017, FBI officials stated they implemented the recommendation by submitting a paper to solicit feedback from users through the Fall 2016 Advisory Policy Board Process. Specifically, officials said the paper requested feedback on whether the face recognition searches of the NGI-IPS are meeting their needs, and input regarding search accuracy.[31] According to FBI officials, no users expressed concern with any aspect of the NGI-IPS meeting their needs, including accuracy.

[29]See FBI, *FBI Information Technology Life Cycle Management Directive*, version 3.0 (August 19, 2005); DOJ, *Systems Development Life Cycle Guidance* (Jan. 2003); and *OMB, Circular No. A-11, Planning, Budgeting, and Acquisition of Capital Assets*, V 3.0 (2015).

[30]National Institute of Standards and Technology, *Face Recognition Vendor Test: NIST Interagency Report 8009* (May 26, 2014).

[31]The FBI's Advisory Policy Board is responsible for reviewing appropriate policy, technical, and operational issues related to the FBI's Criminal Justice Information Services Division programs.

Although FBI's action of providing working groups with a paper presenting GAO's recommendation is a step, FBI's actions do not fully meet the recommendation. FBI's paper was presented as informational, and did not result in any formal responses from users. We disagree with FBI's conclusion that receiving no responses on the informational paper fulfills the operational review recommendation, which includes determining that NGI-IPS is meeting user's needs. As such, we continue to recommend the FBI conduct an operational review of NGI-IPS at least annually.

FBI Has Not Assessed the Accuracy of External Face Recognition Systems

In 2016 we reported that FBI officials did not assess the accuracy of face recognition systems operated by external partners. Specifically, before agreeing to conduct searches on, or receive search results from, these systems, the FBI did not ensure the accuracy of these systems was sufficient for use by FACE Services. *Standards for Internal Controls in the Federal Government* call for agencies to design and implement components of operations to ensure they meet the agencies mission, goals, and objectives, which, in this case, is to identify missing persons, wanted persons, suspects, or criminals for active FBI investigations. As a result, we recommended the FBI take steps to determine whether each external face recognition system used by FACE Services is sufficiently accurate for the FBI's use and whether results from those systems should be used to support FBI investigations.

In comments on our draft report in 2016, and reiterated during recommendation follow-up in 2017, DOJ officials did not concur with this recommendation. DOJ officials stated that the FBI has no authority to set or enforce accuracy standards of face recognition technology operated by external agencies. In addition, DOJ officials stated that the FBI has implemented multiple layers of manual review that mitigate risks associated with the use of automated face recognition technology. Further, DOJ officials stated there is value in searching all available external databases, regardless of their level of accuracy.

We disagree with the DOJ position. We continue to believe that the FBI should assess the quality of the data it is using from state and federal partners. We acknowledge that the FBI cannot and should not set accuracy standards for the face recognition systems used by external partners. We also do not dispute that the use of external face recognition systems by the FACE Services Unit could add value to FBI investigations.

However, we disagree with FBI's assertion that no assessment of the quality of the data from state and federal partners is necessary. We also

disagree with the DOJ assertion that manual review of automated search results is sufficient. Even with a manual review process, the FBI could miss investigative leads if a partner does not have a sufficiently accurate system. The FBI has entered into agreements with state and federal partners to conduct face recognition searches using over 380 million photos. Without actual assessments of the results from its state and federal partners, the FBI is making decisions to enter into agreements based on assumptions that the search results may provide valuable investigative leads. For example, the FBI's accuracy requirements for criminal investigative purposes may be different than a state's accuracy requirements for preventing driver's license fraud.[32] By relying on its external partners' face recognition systems, the FBI is using these systems as a component of its routine operations and is therefore responsible for ensuring the systems will help meet FBI's mission, goals and objectives. Until FBI officials can assure themselves that the data they receive from external partners are reasonably accurate and reliable, it is unclear whether such agreements are beneficial to the FBI, whether the investment of public resources is justified, and whether photos of innocent people are unnecessarily included as investigative leads.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, this concludes my prepared statement. I would be happy to respond to any questions you may have.

[32]We reported in 2012 that 41 states and the District of Columbia use face recognition technology to detect fraud in driver's license applications by ensuring an applicant does not obtain a license by using the identity of another individual and has not previously obtained licenses using a different identity or identities. See GAO, *Driver's License Security: Federal Leadership Needed to Address Remaining Vulnerabilities*, GAO-12-893 (Washington, D.C.: Sept. 21, 2012).

GAO Contact

For questions about this statement, please contact Diana Maurer at (202) 512-8777 or maurerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

Staff Acknowledgments

Individuals making key contributions to this statement include Dawn Locke (Assistant Director), Susanna Kuebler (Analyst-In-Charge), Jennifer Beddor, Eric Hauswirth, Richard Hung, Alexis Olson, and David Plocher. Key contributors for the previous work that this testimony is based on are listed in the previously issued product.

Chairman CHAFFETZ. Thank you.

Mr. Romine, you're now recognized for 5 minutes.

STATEMENT OF CHARLES ROMINE, PH.D.

Mr. ROMINE. Chairman Chaffetz, Ranking Member Cummings, and members of the committee, thank you for the opportunity to discuss the NIST role in standards and testing for facial recognition technology.

Biometric technologies, including face recognition, can provide a means for uniquely recognizing humans based upon one or more physical or behavioral characteristics and can be used to establish or verify identity of individuals.

For decades, biometric technologies were used primarily for homeland security and law enforcement applications. But, today, the marketplace for biometric solutions includes private sector applications, including physical security and retail applications.

NIST has more than five decades of experience improving human identification systems. NIST responds to government and market requirements for biometric standards, including facial recognition technologies, by collaborating with other Federal agencies, law enforcement, industry, and academic partners to support the timely development of scientifically valid fit-for-purpose standards; develop the required conformance testing, architectures, and tools; research measurement, evaluation, and interoperability; and develop common models and metrics for identity management.

NIST work improves the accuracy, quality, usability, interoperability, and consistency of identity management systems and ensures that United States interests are represented internationally. NIST research provides state-of-the-art technology benchmarks and guidance to industry and U.S. Government agencies that depend upon biometrics recognition.

NIST encourages and coordinates Federal agency use of voluntary consensus standards and participation in the development of standards. NIST works with other agencies to coordinate standards issues and priorities with the private sector through industry-led consensus standards-developing organizations.

Starting in 1986 and under accreditation by the American National Standards Institute, or ANSI, NIST has developed a succession of standards for the interchange of biometric data. This standard used around the world facilitates interoperable biometric data exchange across jurisdictional lines and between systems developed by different manufacturers.

From the inception of the International Organization for Standardization's Subcommittee on Biometrics, NIST has led and provided technical expertise to develop international biometric standards that have received widespread international and national market acceptance.

For more than a decade, NIST has been organizing and conducting large biometric technology challenge programs and evaluations. NIST biometric evaluations measure the core algorithmic capability of biometric recognition algorithms and report the accuracy, throughput, reliability, and sensitivity of algorithms to image characteristics, for example, noise or compression, and subject characteristics, for example, age or gender.

NIST biometric evaluations advance the technology by identifying and reporting gaps and limitations of current biometric recognition technologies. NIST evaluations also provide quantitative data to facilitate development of consensus-based standards.

NIST's face recognition vendor tests, or FRVT, assess capabilities of prototype face recognition systems for one-to-many identification and one-to-one verification and provides independent evaluations of commercially available and prototype face recognition technologies.

FRVT provides the U.S. Government with information to assist in determining where and how facial recognition technology can best be deployed. FRVT results also help identify future research directions for the face recognition community. The latest FRVT will measure face recognition performance gains on an ongoing basis to align evaluation and development schedules.

NIST research has helped enhance identity systems, including the Federal Bureau of Investigation's Next Generation Identification system, the Department of Homeland Security Automated Biometric Identification System, the Department of Defense Automated Biometric Identification System, the Department of State biometrics visa program, and the intelligence community systems. For example, virtually all law enforcement biometric collections worldwide use the ANSI NIST standard for data interchange.

NIST is proud of the positive impact it has had in the last 54 years on the evolution of biometrics capabilities. With NIST's extensive experience and broad expertise, both in its laboratories and in successful collaborations with the private sector and other government agencies, NIST is actively pursuing the standards and measurement research necessary to deploy interoperable, secure, reliable, and usable identity management systems.

Thank you for your—for the opportunity to testify in NIST activities in facial recognition and identity management. I'd be happy to answer any questions you may have.

[Prepared statement of Mr. Romine follows:]

Testimony of

Charles H. Romine
Director
Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

Before the

Committee on Oversight and Government Reform
United States House of Representatives

Facial Recognition Technology (FRT)

March 22, 2017

INTRODUCTION

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, I am Chuck Romine, Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). ITL cultivates trust in information technology and metrology through measurements, standards and testing. Thank you for the opportunity to appear before you today to discuss our role in standards and testing for facial recognition technology.

BIOMETRIC AND FACIAL RECOGNITION TECHNOLOGY

Biometric technologies can provide a means for uniquely recognizing humans based upon one or more physical or behavioral characteristics and can be used to establish or verify identity of individuals. Examples of physical characteristics include face, fingerprint, and iris images. An example of behavioral characteristic is an individual's signature. Used with other authentication technologies, such as tokens, biometric technologies can provide higher degrees of security than other technologies employed alone. For decades, biometric technologies were used primarily in homeland security and law enforcement applications, and they are still a key component of these important applications. Over the past several years, the marketplace for biometric solutions has widened significantly and today includes public and private sector applications worldwide, including physical security and retail applications. According to one industry estimate, the global biometrics market revenue will reach $15.1 billion by 2025.[1] Facial recognition technologies, which compare an individual's facial features to available images for identification or authentication, will reportedly reach a market of $9.6 billion by 2022.[2]

NIST Role in Biometric and Facial Recognition Technology

NIST has more than five decades of experience improving human identification systems. NIST responds to government and market requirements for biometric standards, including facial recognition technologies, by collaborating with other federal agencies, law enforcement, industry, and academic partners to:

- support the timely development of scientifically valid, fit-for-purpose standards;
- develop the required conformance testing architectures and testing tools to test implementations of selected standards;
- research measurement, evaluation, and interoperability to advance the use of biometric technologies including face, fingerprint, iris, voice, multi-modal techniques, and emerging identity determination technologies from video; and
- develop common models and metrics for identity management, critical standards, and interoperability of electronic identities.

NIST's work improves the accuracy, quality, usability, interoperability, and consistency of identity management systems and ensures that United States interests are represented in the international arena. NIST research has provided state of the art

[1] "Biometrics Market Forecasts," Tractica, February 2017.
[2] "Facial Recognition Market Report," Allied Market Research, June 2016.

technology benchmarks and guidance to industry, and U.S. Government agencies that depend upon biometrics recognition.

Under the provisions of the National Technology Transfer and Advancement Act (PL 104-113) and OMB Circular A-119, NIST is tasked with the role of encouraging and coordinating federal agency use of voluntary consensus standards in lieu of government unique standards, and federal agency participation in the development of relevant standards, as well as promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities. NIST works with other agencies to coordinate standards issues and priorities with the private sector through consensus standards developing organizations (SDOs) such as the InterNational Committee for Information Technology Standards (INCITS), Joint Technical Committee 1 of the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), the Organization for the Advancement of Structured Information Standards (OASIS), IEEE, the Internet Engineering Task Force (IETF), and other standards organizations such as the International Civil Aviation Organization (ICAO), and the International Telecommunication Union's Standardization Sector (ITU-T). 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'S FACIAL RECOGNITION ACTIVITIES

Voluntary Consensus Standards
Most SDOs are industry-led private sector organizations. Many voluntary consensus standards from those SDOs are appropriate or adaptable for the Government's purposes. OMB Circular A-119 directs the use of such standards by U.S. Government Agencies, whenever practicable and appropriate, to achieve the following goals:

- eliminating the cost to the Federal government of developing its own standards and decreasing the cost of goods procured and the burden of complying with agency regulation;
- providing incentives and opportunities to establish standards that serve national needs, encouraging long-term growth for U.S. enterprises and promoting efficiency, economic competition, and trade; and
- furthering the reliance upon private sector expertise to supply the Federal government with cost-efficient goods and services.

When properly conducted, standards development can result in increased productivity and efficiency in government and industry, greater innovation and competition, expand opportunities for international trade, conserve resources, provide consumer benefit and choice and improve health and safety.

NIST ITL – An American National Standards Institute (ANSI)-accredited SDO
Under accreditation by ANSI, the private-sector U.S. standards federation, NIST continues to develop consensus biometric data interchange standards. Starting in 1986, NIST has developed and approved a succession of data format standards for the interchange of biometric data. The current version of this standard is ANSI/NIST-ITL 1: 2015, *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information*. This standard continues to evolve to support Government applications including law enforcement, homeland security, as well as other identity management applications. This standard, used around the world, facilitates interoperable biometric data exchange across jurisdictional lines and between dissimilar systems developed by different manufacturers.

ISO/IEC Joint Technical Committee 1, Subcommittee 37 (JTC1/SC37) - Biometrics
From the inception of the ISO Subcommittee on Biometrics in 2002, NIST has led and provided technical expertise to develop international biometric standards in this SDO. The subcommittee on Biometrics developed standards have received widespread international and national market acceptance. Large international organizations, such as the ICAO for Machine Readable Travel Documents and the International Labour Office (ILO) of the United Nations for the verification and identification of seafarers, specify in their requirements the use of some of the international biometric standards developed by this subcommittee.

Between 2006 and 2012, JTC1/SC37 published a series of standards on biometric performance testing and reporting. These documents provide guidance on the principles and framework, testing methodologies, modality-specific testing, interoperability performance testing, access control scenarios, and testing of on-card comparison algorithms for biometric performance testing and reporting.

The ICAO has moved the world's passports to a new level of travel document security, data integrity, and identity management. To facilitate the goal of global interoperability, ICAO selected facial recognition as the globally interoperable biometric (listed as mandatory) for machine-assisted identity confirmation for Machine Readable Travel Documents. ICAO selected, as options, the ability to incorporate the specifications for finger and iris. The market research estimates that there will be 817 million ePassports in circulation by 2020, with annual revenue topping $5 billion.[3] These ePassports are issued by 122 countries using the JTC1/SC37 developed standards. This program serves as a model for effective collaboration and cooperation between industry through subcommittees of JTC 1 and the governments of the world through ICAO.

NIST FACIAL RECOGNITION CHALLENGES AND EVALUATIONS
For more than a decade, NIST has been organizing and conducting large biometric technology challenge programs and evaluations for a variety of purposes. NIST biometric evaluations measure the core algorithmic capability of biometric recognition algorithms and report the accuracy, throughput, reliability, and sensitivity of algorithms to image characteristics, for example, noise or compression, and subject characteristics,

[3] "Global ePassport Program Update," Acuity Market Intelligence, 2016.

for example, age or gender. NIST biometric evaluations advance the technology by identifying and reporting gaps and limitations of current biometric recognition technologies. NIST evaluations advance measurement science by providing 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 Multiple Biometric Grand Challenge and Face Recognition Grand Challenge programs to challenge the face recognition community to break new ground solving research problems on the biometric frontier. NIST conducted the Face Recognition Vendor Tests (FRVT) and the Multi-Biometric Evaluation to assess capabilities of prototype face recognition systems for one-to-many identification and one-to-one verification.

Since 2010, NIST has, in cooperation with the United Kingdom National Physical Laboratory and the European Association for Biometrics, organized the biennial International Biometric Performance Testing Conference. This series of conferences accelerate adoption and effectiveness of biometric technologies by providing a forum to discuss and identify fundamental, relevant, and effective performance metrics and disseminating best practices for performance design, calibration, evaluation, and monitoring.

NIST Face Recognition Vendor Testing Program
NIST FRVT provides independent evaluations of commercially available and prototype face recognition technologies. These evaluations provide the U.S. Government with information to assist in determining where and how facial recognition technology can best be deployed. FRVT results also help identify future research directions for the face recognition community. The 2013 FRVT tested facial recognition algorithms submitted by 16 organizations and showed that algorithms made significant improvement since NIST last tested in 2010. NIST defined performance by recognition accuracy—how many times the software correctly identified the photo—and the time the algorithms took to match one photo against large photo data sets.

The latest FRVT, launched February 2017, will measure face recognition performance gains on an ongoing basis. NIST is running the FRVT continually to more closely align evaluation and development schedules. Previous FRVTs were one-time evaluations, performed roughly every three years, that focused on large-scale one-to-many face recognition algorithms from still face photos and from video, along with testing automated methods for estimating pose, expression, and gender.

NIST Face in Video Evaluation Program
Face in Video Evaluation (FIVE) assesses the capability of face recognition algorithms to correctly identify or ignore persons appearing in video sequences. FIVE was an assessment of how well an algorithm could identify a subjects who appears on without explicit direction. The recently released FIVE report enumerates accuracy and speed

of face recognition algorithms applied to the identification of persons appearing in video sequences drawn from six different video datasets.

Human Factors: Facial Forensic Examiners
NIST is researching how to measure the accuracy of forensic examiners matching identity across different photographs. NIST's first study in this effort measured the accuracy of forensic examiners when comparing faces displayed on a computer screen for 30 seconds. The key results of the study showed that trained examiners performed better than untrained individuals and trained examiners' accuracy improved with more time to make a decision. NIST is currently conducting a study to measure performance when trained examiners have access to tools they commonly use.

NIST BIOMETRIC RESEARCH ACTIVITIES ADDRESSING FUTURE CHALLENGES IN FACIAL RECOGNITION TECHNOLOGIES

To better align NIST's evaluation schedule with the pace of face recognition advancement in industry and academia, NIST is currently expanding its face recognition evaluations. 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 face recognition applications. On the research side, following NIST's success and global leadership in fingerprint image quality and iris image quality, NIST plans to initiate research to better understand how to measure face image quality.

IMPACTS OF NIST FACIAL RECOGNITION STANDARDS, TESTING, AND RESEARCH ACTIVITIES

NIST research has provided U.S. Government agencies, with missions that involve biometrics collection and matching, with technology benchmarks and guidance. NIST's research has helped enhance identity systems and operations including the Federal Bureau of Investigation (FBI) Next Generation Identification (NGI) System, the Department of Homeland Security (DHS) Automated Biometric Identification System (IDENT)/US-VISIT, the Department of Defense Automated Biometric Identification System, the Department of State Biometric Visa (BioVisa) Program, and the Intelligence Community systems. For example, virtually all law enforcement biometric collections worldwide use the ANSI/NIST standard. NIST biometric technology evaluations in fingerprint, face, and iris have provided the Government with timely analysis of market capabilities to guide biometric technology procurements and deployments. The FBI has co-sponsored the challenge problems and evaluations, and leveraged this market analysis in its acquisition of NGI system evolution. NIST biometrics research assisted DHS in its transition to ten prints for the US-VISIT program. NIST is currently working with DHS to provide standards guidance, best practices, and analysis in support of designing biometrics-enabled U.S. immigration processes.

CONCLUSION

NIST is proud of the positive impact it has had in the last 54 years on the evolution of biometrics capabilities. With NIST's extensive experience and broad expertise both in its laboratories and in successful collaborations with the private sector and other government agencies, NIST is actively pursuing the standards and measurement research necessary to deploy interoperable, secure, reliable, and usable identity management systems.

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

Chairman CHAFFETZ. Thank you. I do appreciate it.
Mr. Bedoya, you're now recognized for 5 minutes.

STATEMENT OF ALVARO BEDOYA

Mr. BEDOYA. Thank you, Mr. Chairman, Ranking Member Cummings, and members of the committee.

Why should people care about face recognition? Well, historically, law enforcement, when they wanted to identify someone, they had to approach them; they had to talk to them and ask them for ID. Face recognition lets law enforcement identify someone from far away and in secret—and not just one person. The latest generation of this technology will allow law enforcement to scan the face of every man, woman, and child walking in front of a street surveillance camera or police body-worn camera.

This technology raises some serious questions, some basic questions. Do you have the right to walk down the street without the government secretly scanning your face? Is it a good idea to give government so much power with so few limits? Let me say this: with the right protections for privacy, civil liberties, and civil rights, this technology can and will be a tool for good.

Mr. Chairman, our center spent a year studying whether those protections were in place. They are not. No Federal law controls this technology. No court decision limits it. With a few important exceptions, this technology is not under control.

What do I mean by that, "not under control"? Well, start with the databases. Whose faces are in face recognition databases? You would hope that they'd mostly be made up of known or suspected criminals. In fact, just by having a driver's license, one out of two American adults have been enrolled in a criminal face recognition network. That's 125 million people, 51 percent of adults, and 32 out of 44 members of this committee. Twenty-six of those are searchable by FBI.

This has never happened before, not with fingerprints, not with DNA, and most people have no idea that this is happening. That's the databases. Whose faces can you scan and search within those databases? Do you need a warrant to scan someone's face? Do you at least need to reasonably suspect them of a crime, or can you scan anyone?

We surveyed over 100 law enforcement agencies across the country. We found 52 that had used or were using face recognition technology. Not one required a warrant. And in most agencies, as well as the FBI, officials do not need to reasonably suspect someone of a crime before scanning and searching their face.

How is this going to affect free speech? Are you going to a gun rights rally or a protest against the President, for that matter, if the government can secretly scan your face and identify you? This is not a hypothetical. In the course of our investigations, we met a college student who is now in at least two separate face recognition databases after an arrest for peaceful civil disobedience. Now she is so scared that, whenever she goes to a protest, she is afraid to show her face.

What about accuracy? Is there a risk that innocent people will be misidentified and investigated as dangerous criminals? As the GAO just said, yes, there is. The details are unclear, but we know,

for New York, that NYPD system has misidentified at least five people.

Face recognition makes more mistakes than fingerprints, far more mistakes than DNA. And FBI-coauthored research suggests that face recognition is more likely to make mistakes when it looks for the faces of African Americans, women, and young people.

Finally, are there safeguards in place to make sure that these systems are not misused or abused? Unfortunately not. The FBI has run tens of thousands of searches against the faces of law-abiding drivers. But from the GAO's testimony and their reports, we know that none of those searches have been checked for abuse. Those are searches of the DMV driver's license databases.

So, if there is abuse, we would not know it. Mr. Chairman, the safety benefits to this technology are real, but we do not need to choose between safety and privacy. As you know well, the members of this committee have long argued that Americans deserve both.

So I would submit that the question before this committee is not, do we allow face recognition, or do we ban it? I think the question is, how do we put in place checks and balances that let law enforcement do its job while also protecting our rights and our freedoms?

Where might you look for some of these answers? You might look to Ohio, Mr. Jordan's State, for its policy against monitoring protests. You might look to Michigan for their safeguards against misuse and their policy of removing anyone who hasn't been convicted of a crime from a face recognition database. You might look to San Diego for their practice of actually going to elected officials every year and getting approval for their policies. The list goes and on, and all of these proposals are in our report, "The Perpetual Lineup."

Thank you very much for your time. I look forward to your questions.

[Prepared statement of Mr. Bedoya follows:]

GEORGETOWN LAW
Center on Privacy & Technology

Statement of Alvaro Bedoya, Executive Director
Center on Privacy & Technology at Georgetown Law

Before the

U.S. House of Representatives
Committee on Oversight and Government Reform

Hearing on

Law Enforcement's Use of Facial Recognition Technology

Wednesday, March 22, 2017

For more information, contact Alvaro Bedoya at amb420@georgetown.edu or (203) 464-7500, or view our full report on law enforcement face recognition at www.perpetuallineup.org/report.

I. Executive Summary

Face recognition technology lets law enforcement scan people's faces—and identify them—from far away and in secret. This brings real benefits for public safety. Without adequate oversight, however, it also creates real threats to privacy, civil liberties, and civil rights.

Even though *most American adults* are enrolled in a criminal face recognition network, this technology is largely unregulated. No federal law controls it. No court case limits it. A few agencies, in places like California, Michigan, and Washington, have meaningful checks against misuse. In most cases, this technology is not under control.

In 2015, the Center on Privacy & Technology at Georgetown Law began a yearlong evaluation of the privacy, civil liberties, and civil rights protections in face recognition systems used by the FBI and police across the nation. We submitted more than 100 records requests, and received 16,000 pages of responses from 90 agencies. In October, we published our findings in *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, a 150-page report available at www.perpetuallineup.org/report.

A few key takeaways are below.

- **1 in 2 adults are in a criminal face recognition network.** At least 29 states allow criminal face recognition searches of driver's license photos.[1] Over 125 million adults (51%) are in a criminal face recognition network. The FBI can request searches in at least 17 states.[2] Never before—not with fingerprints or DNA—has law enforcement created a national biometric network made up mostly of innocent people.

- **Law-abiding people may be subject to face recognition searches.** No warrants are required for searches of driver's license or other photos. Most agencies, including the FBI, do not require officers to reasonably suspect someone of a crime before using face recognition to ID them. Six major agencies have bought or are exploring real-time face recognition on live video. This technology can scan the face of every man, woman or child who passes in front of a street camera. Eventually, this technology could be used to scan every face that passes by a police body-worn camera. It's unclear if the FBI is exploring or using real-time face recognition.

- **Agencies are not taking steps to protect free speech.** It appears that face recognition has been used to ID people attending protests. An FBI presentation

[1] For a list of 26 of those 29 states, *see* Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, 28 (2016), *available at* https://www.perpetuallineup.org/report (hereinafter "*The Perpetual Line-Up*"). Since publication, we have verified that Alaska, Idaho and New Jersey also allow law enforcement searches of license photos.
[2] According to a 2016 GAO report, the FBI can run or request searches of 16 states' driver's license photos. Our Center verified that FBI field agents in Florida can also request searches of driver's license photos in that system. GAO-16-267, at 47–48; *The Perpetual Line-Up*, at 25.

suggests the use of face recognition at political rallies. While the Privacy Act would bar the FBI from using this technology to track political speech, the FBI recently moved to exempt itself from lawsuits for violations of that provision. Of the dozens of agencies we surveyed, only one, in Ohio, clearly restricted face scans at protests.

- **Face recognition makes mistakes. It may make *more* mistakes for searches of African Americans and women.** When it was implemented, roughly one in seven searches of the FBI's system returned a list of entirely "innocent" candidates. FBI co-authored research suggests that face recognition may be less accurate on African Americans and women. In October, a coalition of 52 civil rights and civil liberties groups asked the Department of Justice to investigate racial bias in face recognition.

- **Agencies are keeping critical information from the public.** After consistently failing to comply with mandatory transparency laws, the FBI has proposed to exempt its system from Privacy Act provisions on public access and judicial review. Of the police agencies we surveyed, less than 10% had a public policy explaining how they use face recognition. Only one agency submitted its policy for legislative approval.

- **Major face recognition systems, including the FBI's, are not regularly audited for misuse.** Only 17% of the agencies surveyed indicated that they logged and audited officers' face recognition searches for misuse. Only one, in Michigan, provided documentation of a functional audit regime. The Government Accountability Office found that in the first 4.5 years of operation, the FBI never audited its use of face recognition.

Since the 1968 passage of the Wiretap Act, Congress has passed laws that *allow* law enforcement to use advanced technology to investigate crime, while simultaneously protecting Americans' basic freedoms. The debate before this Committee is *not* whether to ban law enforcement face recognition or allow it. Instead, the question before us is how to create a system of checks and balances that lets us reap the law enforcement benefits of face recognition, while also protecting American liberty.

II. Why should you care about law enforcement face recognition?

Historically, when law enforcement wanted to identify someone, they had to approach that person and ask for identification. Even when police identified someone using DNA or fingerprints, this was generally a targeted process where a single person was identified as part of an investigation, usually through an in-person or on-site interaction. Think of a police officer rolling a suspect's fingers across an inkpad, or an investigator collecting a hair sample from a crime scene.

Face recognition can be used in a similar way. An officer in the street may use a smartphone face recognition app to identify someone in the course of a field stop; a jail can use it to verify a detainee's identity from his mug shot. In its more advanced uses, however, face recognition lets law enforcement identify people from far away and in secret. It also lets them remotely identify large *groups* of people, not just the target of an

investigation.[3] Think of a telephoto lens being used to surreptitiously photograph and ID the people in a crowd, or a surveillance camera that scans every face passing by.

These tools will help law enforcement. Left unchecked, however, law enforcement face recognition creates profound questions about the future of our society. Should this technology be targeted at serious criminals and terrorists? Or should it be used to scan the face of anyone, at any time? Should face recognition databases be limited to criminals? Or should they include the faces of every man, woman, and teenager with a driver's license? Do you have the right to walk down your street without having your face scanned?

In the past, Congress and the states have answered these kinds of questions through legislation. In the absence of any comprehensive federal or state statutes—or any court decisions, for that matter—in most cases, the full extent of privacy and civil liberties protections depends on the policies voluntarily adopted by law enforcement agencies. Our investigation aimed to identify those policies and evaluate their impact.

III. How does the FBI use face recognition?

The FBI has devoted substantial resources to face recognition. FBI face recognition searches of state driver's license photos are almost six times more common than federal court-ordered wiretaps.[4]

The FBI has two primary roles with respect to face recognition. First, the FBI hosts a database of at least 24.9 million mugshots, the Next Generation Identification Interstate Photo System (NGI-IPS), which is searchable by the FBI and a dozen state agencies.[5]

Second, the FBI is also an active *user* of the technology. Its Facial Analysis, Comparison, and Evaluation Services unit (FACE Services) runs or requests criminal face recognition searches of a network of databases that together contain 411.9 million face photos. This network includes Department of State visa photos and 16 states'

---

[3] Some uses of face recognition are riskier than others. For a simple taxonomy of less risky vs. more risky uses, see *The Perpetual Line-Up* at 16–22, or visit https://www.perpetuallineup.org/risk-framework.

[4] *The Perpetual Line-Up*, at 79, n. 68 (2016) ("From 2011 to 2015, federal judges authorized a total of 6,304 wiretaps. *See* United States Courts, Wiretap Report 2015, http://www.uscourts.gov/statistics-reports/wiretapreport-2015 (last updated Dec. 31, 2015); United States Courts, Wiretap Report 2014, http://www.uscourts.gov/statistics-reports/wiretap-report-2014 (last updated Dec. 31, 2014); United States Courts, Wiretap Report 2013, http://www.uscourts.gov/statistics-reports/wiretap-report-2013 (last updated Dec. 31, 2013); United States Courts, Wiretap Report 2012, http://www.uscourts.gov/statistics-reports/wiretap-report-2012 (last updated Dec. 31, 2012); United States Courts, Wiretap Report 2011, http://www.uscourts.gov/statistics-reports/wiretap-report-2011 (last updated Dec. 31, 2011).").

[5] U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy, Table 3 (May 2016) *available at* https://www.gao.gov/products/GAO-16-267 (hereinafter "GAO-16-267"). According to the FBI Criminal Justice Information Services Annual Report from 2016, there are now a total of 51 million facial images in NGI, including criminal and civil photos, up from 30 million total facial images reported by GAO as of December 2015. CJIS, Annual Report 2016, 16 (2016), *available at* https://www.fbi.gov/file-repository/2016-cjis-annual-report.pdf/view.

driver's license photos.[6] (Our research revealed that the FBI field offices in Florida can also conduct face recognition searches of that state's driver's license photos, but these searches are not run through FACE Services.)[7]

The GAO found that from August 2011 to December 2015, FACE Services ran 36,420 searches of those 16 states' driver's photos. These searches produced only 210 likely candidates for investigation.

The FBI is in a unique position to influence how law enforcement uses face recognition, and ensure that police departments adopt protections for privacy, civil liberties, and civil rights. It could model best practices to be adopted by state and local police departments, or condition access to its database (NGI-IPS) on agency adoption of those best practices. As the following section shows, this is an untapped opportunity.

III. Problems and Recommendations.

A. Face recognition is *not* targeted at criminals. It affects millions of law-abiding Americans.

Since the ratification of the Fourth Amendment in 1791, Americans have agreed that law enforcement should not invade our privacy absent a well-founded suspicion of criminal wrongdoing. As a result, law enforcement generally treats known and suspected criminals very differently from law-abiding people.

Law enforcement use of face recognition does not abide by that principle. It subjects millions of Americans to a powerful—and error-prone—surveillance technology.

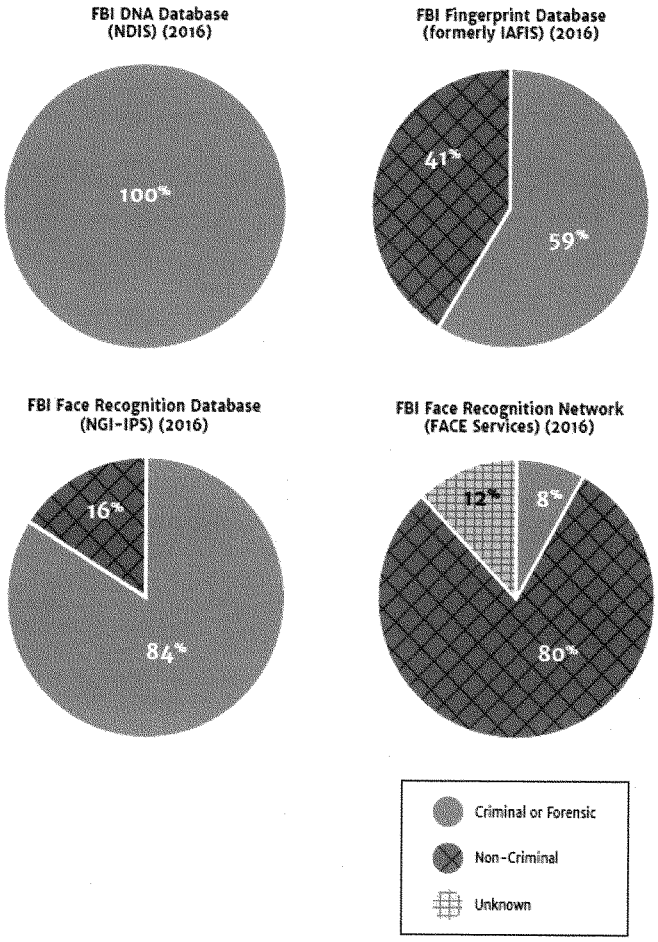
1. Face recognition *databases* are not limited to criminals.

Teenagers anxiously wait for the day when they will be old enough to go to the Department of Motor Vehicles, take a test, stand for a photo, and then receive a learner's permit. What if every teen in America was then asked to submit their fingerprints for future criminal investigations by the FBI or the state police?

Many people would be outraged. Yet our research shows that 29 states allow federal and state law enforcement to use face recognition technology to run or request searches of their drivers' faces, much like they would criminals' fingerprints.[8] As of 2014, there were 125,392,814 licensed drivers aged 18 or older in those states. Based on Census figures, we can estimate that at least 51% of all American adults are in a criminal face recognition network.[9]

---

[6] Recently, FACE Services has also been able to request searches of U.S. citizen passport photos through a pilot program. *See* GAO-16-267 at 7, n. b.
[7] *The Perpetual Line-Up*, at 25.
[8] *See* note 1 for information on where to find a list of these states.
[9] *See* Federal Highway Administration, *U.S. Department of Transportation, Highway Statistics* (Sept. 2015), *available at* http:// www.fhwa.dot.gov/policyinformation/statistics/2014/pdf/ dl22.pdf; *see* U.S. Census Bureau, *Annual Estimates of the Resident Population for Selected Age Groups by Sex for the*



The vast majority of these people have no idea that this is happening. We're not aware of any effort in these states to actually notify drivers that their faces will be searched as part of criminal investigations. In fact, of the 29 states, only two have laws that formally authorize law enforcement face recognition scans of their driver's license

---

United States, States, Counties, and Puerto Rico Commonwealth and Municipios: April 1, 2010 to July 1, 2014: 2014 Population Estimates, available at http://factfinder.census.gov/bkmk/table/1.0/en/PEP/2014/PEPAGESEX.

photos.[10] In most others, law enforcement appears to rely on readings of driver's privacy laws that were written before the advent of face recognition.

As the figure in the previous page shows,[11] law enforcement biometric databases have been typically populated exclusively or primarily by criminal or forensic samples. The FBI's National DNA Index System, or "NDIS," is almost exclusively composed of DNA profiles related to criminal arrests or forensic investigations. Over time, the FBI's fingerprint database has come to include non-criminal records, including the fingerprints of immigrants and civil servants. However, even when one considers the addition of non-criminal fingerprint submissions, the latest figures available suggest that the fingerprints held by the FBI are still primarily drawn from arrestees.

FBI FACE Services bucks this trend. By searching 16 states' driver's license databases, photos from visa applications, and Americans' passport photos, the FBI has created a network of databases that is overwhelmingly made up of *non*-criminal entries.

This is unprecedented. Never before has law enforcement created a national biometric database—or network of databases—that is primarily made up of law-abiding people.

2. Face recognition *searches* are not limited to criminals.

The above section explains who is in face recognition databases. Whose faces can officers scan and search for *against* those databases? Can they search only for suspected criminals? Or can they effectively scan and search anyone? In most agencies we surveyed—and in the FBI—the answer appears close to the latter.

Of the 90 agencies that provided responsive documents to our survey, 52 state and local law enforcement agencies are now using or previously used face recognition technology. None of those agencies appears to require officers to get a warrant before using face recognition to identify someone, even when searching driver's license photos. That said, 12 of those 52 clearly require that officers either reasonably suspect someone of a crime or actually have probable cause to think that he or she was engaged in criminal conduct. These include agencies in California, Iowa, Hawaii, Maine, Michigan, New Mexico, and Washington.

Unfortunately, the remaining 40 agencies—and the FBI—either apply a lower standard or may not have any standard at all.

---

[10] *See* Mich. Comp. Laws Ann. § 28.248 ("Biometric data obtained under a law or rule for noncriminal identification purposes may be used for criminal identification purposes unless prohibited by law or rule."); Tex. Transp. Code § 521.059 ("The [Department of Motor Vehicles] shall use the image verification system established under this section ... to aid other law enforcement agencies").

[11] *See The Perpetual Line-Up,* at 77, n. 49. These numbers reflect those found by the GAO as of December 2015. FBI CJIS has since provided an updated total number of images in NGI-IPS—51 million—but the criminal vs. civil breakdown has not been published. *See* note 3.

FBI FACE Services can run a face recognition search on mere "allegation or information." In other circumstances, they can run a face recognition search on anyone so long as they can point to a non-arbitrary criminal justice or national security purpose.[12]

One state runs 8,000 monthly searches on the faces of seven million drivers—without requiring that officers have even a reasonable suspicion before running a search. In fact, while officers are told to ask for consent before taking someone's photo to scan their face, they are expressly told that they can take photos without consent, and are in fact "encouraged to use [face recognition] whenever practical."[13]

There are situations when face recognition can and should be used to identify non-criminals. Missing people and the victims of crimes, for example, may be unable to safely identify themselves. Others argue that the technology should be used to identify witnesses. But these are exceptions that could be made to an otherwise firm rule.

Changes in technology are likely to make suspicionless searches even more common. The most advanced use of face recognition, real-time face recognition on live video, scans the face of every man, woman, or child that passes in front of a surveillance camera in or close to real-time. Based on documents and public statements, agencies in Chicago, Dallas, Los Angeles, New York and West Virginia either have bought this technology, have announced plans to use it, or are actively exploring it. (An agency in Seattle bought the technology, but has barred real-time scans in its use policy.) It is unclear if the FBI has acquired or is using this technology, or if it is exploring it.

In the future, your face may also be scanned whenever you pass in front of a police officer wearing a body camera. A November survey commissioned by the Department of Justice verified that body-worn camera vendors are "developing and fine-tuning" face recognition features, and identified ten out of 38 vendors that currently allow face recognition in some form or include an option for the software to be used later.[14] Senior executives at Taser, the world's largest manufacturer of body-worn cameras, have

---

[12] FBI face recognition searches run by FACE Services can be run on "the images of persons associated with open assessments and investigations." Full investigations can be opened only "when there is 'an articulable factual basis' of possible criminal or national threat activity"—a standard approaching reasonable suspicion. But preliminary investigations can be opened on mere "allegation or information." And, so long as they are not clearly arbitrary or speculative, assessments can be opened "to detect, obtain information about, or prevent or protect against federal crimes or threats to national security"—an even broader standard. Federal Bureau of Investigation, *Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit,* 2, n. 1–2 (2015), *available at* https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit.

[13] *The Perpetual Line-Up*, at 13.

[14] Vivian Hung, Steven Babin, & Jacqueline Coberly, *A Market Survey on Body Worn Camera Technologies*, National Institute of Justice, 8-404 (2016), available at: https://www.ncjrs.gov/pdffiles1/nij/grants/250381.pdf.

repeatedly said that they expect body cameras to eventually scan faces and recognize individuals in real-time.[15]

Is the public ready for every pedestrian's face to be scanned? Are we willing to allow a tool designed for police oversight to be used for public surveillance?

3. Face recognition searches are not limited to *serious* crimes.

Historically, the most invasive police technologies have been focused on the most dangerous criminals. For example, when Congress passed the Wiretap Act in 1968, it did not allow wiretaps of oral and phone communications for *all* criminal investigations. Rather, it restricted wiretaps of those communications to investigations of certain serious offenses.[16] Under the Wiretap Act, the FBI or the police can't wiretap jaywalkers or bad drivers; it can wiretap murderers and drug traffickers.

No such principle applies in face recognition. Neither the FBI nor any of the 52 agencies known to have used face recognition clearly restrict face recognition searches to more serious crimes. Only one, in Nebraska, limited its use to a certain kind of offense (identity theft).[17]

4. Recommendations.

There is a range of reforms that the FBI and legislators could pursue to address these issues.

(1) Searches of driver's licenses should be strictly limited. Mugshots, not driver's licenses, should be the default databases for face recognition systems. The FBI and police departments should not run or request face recognition searches of driver's license photos unless (a) the state has expressly authorized this practice, and (b) residents of that state are clearly notified.

(2) Ban suspicionless searches. Limit secret searches to serious crimes. Law enforcement should not be able to scan and search the face of anyone at any time. When police encounter someone in person, they should have reasonable suspicion before they use face recognition to identify that individual. After-the-fact searches that occur outside of the public eye should be restricted to felonies. Searches of driver's license photos should require a warrant, and should be limited to investigations of serious crimes.

---

[15] *See* Alex Pasternack, "Police Body Cameras Will Do More Than Just Record You," *Fast Company*, March 3, 2017; Karen Weise, "Will a Camera on Every Cop Make Everyone Safer? Taser Thinks So," *Bloomberg Businessweek*, July 12, 2016.

[16] 18 U.S.C.A. § 2516.

[17] *The Perpetual Line-Up*, at 83 n. 145 (citing Nebraska State Patrol, Memorandum of Understanding between the Nebraska State Patrol and the Nebraska DMV, Document p. 009190, available at: https://drive.google.com/drive/u/0/folders/0B-MxWJP0ZmePMXRfWVZiakYyQjg).

(3) Real-time face recognition should be used only in emergencies and with a court order comparable to that required for wiretaps. If deployed pervasively on surveillance video or police body-worn cameras, real-time face recognition will redefine the nature of public spaces. In the words of the Department of Justice, "[a]gencies that explore this integration... should proceed very cautiously and should consult with legal counsel and other relevant stakeholders."[18] Communities should carefully weigh whether to allow real-time face recognition. If they do, it should be used as a last resort to intervene in only life-threatening emergencies. Orders allowing it should require probable cause, specify where continuous scanning will occur, and cap the length of time it may be used.

Many of these recommendations could be unilaterally implemented by the FBI. For example, for recommendation (2), the FBI could limit access to its face recognition database (NGI-IPS) to agencies that meet these standards.

B. Face recognition may threaten free speech.

Will Americans attend a peaceful political rally if they know that their government can track and identify them from afar? Will they go about their daily lives the same way? Will they visit psychiatrists, Alcoholics Anonymous meetings, or marriage counselors, when they need to?

The impact of law enforcement face recognition on the freedom of speech, association, and assembly, is obvious. To its credit, the FBI has itself recognized the chilling effect of law enforcement face recognition, particularly when it is used to secretly identify people from afar. A Privacy Impact Assessment, drafted in 2011 by DHS in consultation with experts from the FBI and a number of state police agencies, considered the effects of law enforcement face recognition on the "erosion or compromise of anonymity." The document recognizes that "surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition."

The Assessment encourages that law enforcement policies include clear provisions "concerning the appropriate use of a facial recognition field identification tool in areas known to reflect an individual's political, religious or social views, associations, or activities." A specific recommendation: "[T]he collection of long range lens photographs should be limited to instances directly related to criminal conduct or activity."[19]

---

[18] Department of Justice, Bureau of Justice Assistance, *Body-worn Camera Toolkit: Body-worn Cameras Frequently Asked Questions*, 44 (2015), available at: https://www.bja.gov/bwc/pdfs/BWC_FAQs.pdf.

[19] The International Justice and Public Safety Network, *Privacy Impact Assessment: Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field* (June 30, 2011), Document pp. 016625–016693, available at: https://drive.google.com/open?id=0B-MxWJP0ZmePVW9vTnpacU5hME0.

1. Law enforcement agencies do not have adequate protections in place for free speech and assembly.

It's unclear how closely the FBI is following its own guidance. The vast majority of police departments are not.

In a 2012 Senate hearing, Senator Al Franken, then Chairman of the Senate Subcommittee on Privacy, Technology and the Law, confronted the FBI about an agency PowerPoint presentation showing how face recognition could be used to identify people attending the 2008 presidential campaign rallies for then-senators Barack Obama and Hillary Clinton. In response, an FBI representative clarified that the agency had "absolutely no intention" of engaging in that kind of activity.[20]

Years later, FBI guidance to police departments searching the FBI's face recognition database (NGI-IPS) requires those agencies to adopt face recognition use policies that "expressly prohibit collection of photos in violation of an individual's 1st and 4th Amendment rights." We reviewed the policies of four agencies that search that database, and none of them included that language. It's unclear if a similar prohibition exists for FBI FACE Services.

Arguably, the FBI would be prohibited from using face recognition to track individuals' political beliefs outside the context of a lawful law enforcement activity. This stems from section (e)(7) of the Privacy Act, a provision that was adopted in the wake of Watergate and the abuses J. Edgar Hoover era.[21] However, in May 2016, the FBI proposed to immunize its face recognition database (NGI-IPS) from lawsuits alleging violations of that provision.[22]

Of the 52 state and local law enforcement agencies that used face recognition, only one agency, in Ohio, expressly addressed the use of face recognition on First Amendment activities in its use policy.[23]

While the exact circumstances are unclear, late last year, documents obtained by the ACLU suggested that the Baltimore County Police had used face recognition, paired with social media monitoring from Geofeedia, to identify protesters in the spring 2015 protests after the death of Freddie Gray.[24] Apparently, the Baltimore County Police

---

[20] *See* United States. Cong. Sen. Subcommittee on Privacy, Technology of the Law, Sen. Committee on the Judiciary, What Facial Recognition Technology Means for Privacy and Civil Liberties, July 18, 2012, 112th Cong. 2nd sess..

[21] 5 U.S.C.A. § 552a (e)(7) ("Each agency that maintains a system of records shall ... maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity").

[22] Federal Bureau of Investigation, Department of Justice; Privacy Act of 1974; Implementation, 81 Fed. Reg. 27,288, 27,289 (May 5, 2016) (codified at 28 C.F.R. Pt. 16) (item (3) proposes to exempt NGI from subsection (g) of the Privacy Act).

[23] *The Perpetual Line-Up*, at 44, 85 n. 171.

[24] *See* Kevin Rector and Alison Knezevich, "Social media companies rescind access to Geofeedia, which fed information to police during 2015 unrest," *Baltimore Sun* (Oct. 11, 2016).

Department ran photos of individuals posted to social media from the times and locations of the protests through face recognition to identify individuals with warrants out for their arrest.[25]

2. Recommendations.

Use of face recognition at protests should be highly restricted, and the use of the technology to track people on the basis of their political or religious beliefs or their race or ethnicity should be banned. The Ohio Bureau of Criminal Investigation's rule states:

> Law enforcement may not employ this technology to conduct dragnet screening of individuals, nor should it use it to facilitate mass surveillance of places, groups or activities unless doing so furthers an official law enforcement activity. For example, it would not be appropriate for law enforcement to use facial recognition technology to conduct surveillance of persons or groups based solely on their religious, political or other constitutionally protected activities or affiliations unless doing so furthers an official law enforcement activity.[26]

Agencies would do well to adopt this prohibition.

C. Face recognition makes mistakes. Those mistakes may be biased.

Agencies that use face recognition often describe it to the public as highly accurate—and race neutral. They sometimes say that face recognition "does not see race."[27]

In reality, face recognition systems make mistakes. They make *more* mistakes when they're used more aggressively. Research suggests that they also may make more mistakes when used to identify African Americans, women, and young people.

When face recognition systems make mistakes, everyone loses: real criminals will remain free, and innocent people may be investigated.

---

[25] In describing the partnership, Geofeedia referred to the individuals as "rioters," but the police department has not released any information on the crimes these individuals were charged with, or whether they were correctly identified. *See* Geofeedia, "Baltimore County Police Department and Geofeedia Partner to Protect the Public During Freddie Gray Riots" (made public Oct. 11, 2016 by ACLU).

[26] Ohio Bureau of Criminal Investigation, "To Be Added 2016 Date TBD," Document p. 009218, available at: https://drive.google.com/open?id=0B-MxWJP0ZmePX3JVR3huTmVxSjA, (note this language was implemented in 2016 and replaced language that did not address the issue of the use of face recognition on First Amendment activities).

[27] *See* Seattle Police Department, "Booking Photo Comparison System FAQs" (stating that the Seattle PD's system "does not see race, sex, orientation or age." In 2009, Scott McCallum then-systems analyst for the Pinellas County Sheriff 's Office face recognition system, made the same claim to the *Tampa Bay Times*. "[The software] is oblivious to things like a person's hairstyle, gender, race or age, McCallum said." " Kameel Stanley, "Face recognition technology proving effective for Pinellas deputies," *Tampa Bay Times*, July 17, 2009.

1. Many face recognition systems suffer from accuracy problems. Inaccuracy is likely higher for African Americans and others.

In an initial test of the FBI's face recognition database (NGI-IPS), where the supposed perpetrator was *known to be in the database*, roughly one in seven searches of the system returned a list of entirely "innocent" candidates.[28] This test was done on a sample database of roughly one million photos. The actual database is more than 20 times larger than that, and errors tend to increase with database size.

These mistakes do not appear to be evenly distributed across uses and populations.

Face recognition performs well with good lighting, high resolution photos, and cooperative subjects—someone who voluntarily stands for a police officer's photo, or a DMV or passport snapshot. Face recognition performs poorly with low lighting, low resolution, and "non-cooperative subjects," such as when face recognition is used to identify someone from a security camera still or a real-time video, and other scenarios where a person doesn't realize that he or she is being recorded or is actively trying to avoid it.[29]

Mistakes are also likely not evenly distributed across the population. While more research in this field is necessary, a prominent 2012 study co-authored by an FBI expert found that several leading algorithms performed worse on African Americans, women, and young adults than on Caucasians, men, and older people, respectively.[30]

All three of the algorithms were 5 to 10% less accurate on African Americans than Caucasians. In one instance, a commercial algorithm failed to identify Caucasian subjects 11% of the time but did so 19% of the time when the subject was African American—a nearly twofold increase in failures. In more concrete terms: If the perpetrator of a crime were African American, the algorithm would be almost twice as likely to miss the perpetrator entirely, causing the police to lose out on a valuable lead.

Depending on how a system is configured, this effect could also lead the police to misidentify the suspect and investigate the wrong person. Many systems return the top few matches for a given suspect no matter how bad the matches themselves are. If the suspect is African American rather than Caucasian, the system is more likely to erroneously fail to identify the right person, potentially causing innocent people to be bumped up the list—and possibly even investigated. Even if the suspect is simply

---

[28] GAO-16-267, at 26 ("86 percent of the time, a match to a person in the database was correctly returned within a candidate list of 50 potential matches.").

[29] Patrick J. Grother, Mei L. Ngan, George W. Quinn, *Face In Video Evaluation (FIVE) Face Recognition of Non-Cooperative Subjects*, NIST Interagency/Internal Report (NISTIR) – 8173, 6, 62-63 (Mar. 6, 2017), available at: https://www.nist.gov/publications/face-video-evaluation-five-face-recognition-non-cooperative-subjects)/.

[30] *See* Brendan F. Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 IEEE Transactions on Information Forensics and Security 1789, 1797 (2012), available at: http://ieeexplore.ieee.org/document/6327355/).

knocked a few spots lower on the list, it means that, according to the face recognition system, innocent people will look like better matches.

Perversely, due to disproportionately higher arrest rates among African Americans, face recognition may be least accurate for those it is most likely to affect: African Americans. The civil rights community has taken notice. In October, a coalition of 52 civil rights and civil liberties groups publicly called on the Department of Justice Civil Rights Division to investigate bias in law enforcement face recognition systems.[31]

2. Recommendations.

(1) Systems should be regularly and publicly tested for accuracy and bias. Law enforcement agencies, including the FBI, should periodically publicly test their systems (in operational conditions) for accuracy and bias on the basis of race, gender, and age. Congress and state legislatures can condition funding for federal or state face recognition systems on the release of this information.

(2) NIST should conduct regular tests for bias and develop resources for outside testing. The National Institute of Standards and Technology already conducts independent accuracy tests on face recognition algorithms, and has increased testing for face recognition on non-cooperative subjects and real-time video. NIST should build on this progress by increasing the frequency of its accuracy tests, and incorporating into those regular tests evaluations of race, age, and gender bias. NIST can facilitate private, in-house testing for bias by developing and distributing datasets of photos that reflect the full diversity of the American population.

D. Most face recognition systems are not audited to prevent misuse.

Once you establish a rule, how do you know if anyone has broken it? For police surveillance systems, several of the problems identified in our report could be at least partly addressed by internal audits to prevent and identify misuse and abuse. Unfortunately, these kinds of audits are rare.

1. Few agencies have a policy of conducting use audits. Of those, even fewer may actually conduct them.

Of the 52 agencies that we identified had used face recognition, only one, the Michigan State Police, actually provided documentation verifying that audits are, in fact, conducted.[32]

Several agencies, including agencies that enrolled millions of drivers' photos into face recognition networks, openly told us that they did not audit face recognition searches. In fact, only nine (17%) of the 52 agencies expressly indicated that they audit

[31] *See* Craig Timberg, "Racial profiling, by computer? Police facial ID tech raises civil rights concerns," *The Washington Post*, October 16, 2017.
[32] *The Perpetual Line-Up*, at 90 n. 265.

their employees' use of the face recognition system for misuse. The FBI FACE Services unit also has an audit policy.[33]

Of these agencies, however, at least some of them do not actually conduct audits or have gone for long periods of time without conducting one. FACE Services began running or requesting face recognition searches in 2011, the same year that the FBI face recognition database (NGI-IPS) began processing search requests from state and local users. As of the May 2016 GAO report, however, FBI had never audited any of those searches[34]—even though in 2012, an FBI representative had assured the Senate Judiciary Subcommittee on Privacy, Technology and the Law that these audits would be conducted.[35] It would appear that of the 36,420 FBI face recognition searches of driver's license photos, not one was audited to prevent misuse.

2. Recommendations.

(1) The FBI must audit state and local searches of the NGI-IPS database, and its own FACE Services searches of FBI and external databases. This echoes a recommendation in the GAO report.

(2) State and local police departments should regularly audit their use of face recognition to prevent and identify misuse and abuse. Law enforcement agencies should audit their officers' use of face recognition, regardless of whether the agency runs its own system or accesses another's.

E. Face recognition systems are shrouded in secrecy.

Face recognition is too powerful to be secret. Yet our investigation revealed several states that enrolled all of their drivers into a law enforcement face recognition network without any meaningful notice. The FBI, for its part, has also fallen short on its transparency obligations to the American public. This is a problem.

1. Many law enforcement agencies are not transparent about using face recognition.

The E-Government Act and the Privacy Act mandate that the FBI publish a System of Records Notice or a Privacy Impact Assessment when the agency starts to maintain—or significantly modifies—a database like the FBI face recognition database

---

[33] *The Perpetual Line-Up*, at 90 n. 261.

[34] GAO-16-267, at 25.

[35] *See What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing before the Subcomm. on Privacy, Technology & the Law of the S. Comm. on the Judiciary*, 112th Cong., 10–11 (2012) ("One of the things that the MOUs that we sign with the agencies that are going to access the system require is an audit process, so the local agencies are required to audit the use of the system on an annual basis to detect any type of misuse. And then, in addition to that, within our FBI CJIS Division we have an audit unit that goes out and does triennial audits of the same agencies ... a double-check on the audits, as well as to be sure that the audit processes are in place and being done effectively.").

(NGI-IPS).[36] In 2011, the FBI gave select state police departments the ability to run face recognition on photos in the FBI's database. Yet the FBI didn't publish a Privacy Impact Assessment about the program until 2015. Even though the FBI's face recognition database itself was launched in 2008, the FBI didn't publish a System of Records Notice about it until 2016.[37]

These are not obscure bureaucratic filings. They are the means through which the American public can learn about new government tracking technology and hold the government accountable for going too far. Instead of working to address these shortcomings, the FBI is now proposing to exempt its Next Generation Identification system, which includes its face recognition database (NGI-IPS), from provisions of the Privacy Act that guarantee members of the public access to records that identify them, information about the sharing of these records, and judicial review.[38]

Police departments also generally tell the public very little about their use of face recognition. Large, populous states have enrolled all of their drivers—millions of residents—into law enforcement face recognition networks without providing them any meaningful notice.[39]

Only four of the agencies we surveyed—the San Diego Association of Governments (SANDAG), the Honolulu Police Department, the Michigan State Police, and the Seattle Police Department—make their face recognition use policies available to the public.[40] Only one of those agencies, SANDAG, actually submits its face recognition use policy to a legislative body for approval.[41] We are also aware of only one agency that regularly reports to the public how frequently face recognition is used.[42]

Communities aren't the only ones in the dark. In criminal litigation, prosecutors are required to disclose to defense counsel any evidence that may exculpate the accused; those disclosures are referred to as "*Brady* disclosures" or "*Brady* evidence," after the Supreme Court case that mandated those productions.[43] One public defender reported to us that in the 15 years that that his county's face recognition system had been operational, his office had never received any face recognition information as part of a *Brady* disclosure. In an interview, he suggested that if a face recognition system ever

---

[36] M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003); 5 U.S.C. § 552a(e)(4) (requiring agencies to publish any "establishment or revision of" a system of records in the Federal Register).

[37] *See* Center on Privacy & Technology et. al., *Comment on NPRM 81 Fed. Reg. 27288* (July 6, 2016), https://www.regulations.gov/document?D=DOJOPCL-2016-0008-0114.

[38] *See* 5 U.S.C. § 552a; Implementation, 81 Fed. Reg. 27288, 27829 (proposed May 5, 2016) (to be codified at 28 C.F.R. pt. 16); *see also* Center on Privacy & Technology et. al., *Comment on NPRM 81 Fed. Reg. 27288* (July 6, 2016), https://www.regulations.gov/document?D=DOJOPCL-2016-0008-0114 (explaining impact of proposed exemption of FBI's NGI System from key Privacy Act accountability provisions).

[39] *The Perpetual Line-Up*, at 58, 132.

[40] *The Perpetual Line-Up*, at 89-90 n. 251.

[41] *The Perpetual Line-Up*, at 90 n. 256.

[42] *The Perpetual Line-Up*, at 90 n. 252.

[43] *See* Brady v. Maryland, 373 U.S. 83 (1963).

identified someone other than a criminal defendant as a potential suspect in that defendant's case, public defenders would have a right to know.[44]

2. Recommendations.

(1) Law enforcement use of face recognition should be transparent and accountable to the public. Agencies should publicly disclose their use of face recognition, consult with community and civil society groups in crafting policies for how they will use it, post those policies publicly, and obtain legislative approval for them. Congress and state legislatures could condition funds for these systems on these benchmarks.

(2) Law enforcement use of face recognition should be subject to public reporting requirements. Any law enforcement agency using face recognition should be required to annually and publicly disclose information directly comparable to that required by the Wiretap Act.[45] This would include:

a. the number of face recognition searches run;
b. the nature of those searches;
c. the crimes that those searches were used to investigate;
d. the arrests and convictions that resulted from those searches;
e. the databases that those searches accessed; and
f. for real-time video surveillance, the duration and approximate location of those searches.

(3) Agencies should disclose the use of face recognition as part of *Brady* evidence.

Disclosing the use of face recognition pre-trial in criminal proceedings may be an important procedural protection for criminal defendants. It will also allow law enforcement face recognition to receive judicial scrutiny. To date, no state or federal court has evaluated the impact of face recognition technology on Fourth or First Amendment rights. *Brady* disclosures could change that.

IV. Conclusion

In regulating law enforcement use of face recognition, will we blunt our ability to respond quickly and effectively to threats to our safety? I believe that the answer to this question is clearly "no." Face recognition can and should be used to respond to serious crimes and public emergencies. It should not be used to scan the face of any person, at any time, for any crime. It is possible to create a regulatory scheme to enforce that difference.

We do not need to choose between safety and privacy. Americans deserve both.

---

[44] *The Perpetual Line-Up*, at 90 n. 249-50.
[45] *See* 18 U.S.C. § 2519.

Chairman CHAFFETZ. Thank you.

Mr. Hutchinson, you're now recognized for 5 minutes.

STATEMENT OF BENJI HUTCHINSON

Mr. HUTCHINSON. Good morning, Chairman Chaffetz, Ranking Member Cummings, and committee members. Thank you for inviting me to testify today on behalf of IBIA.

I have 13 years of experience in the biometrics and identity tech industry. I've supported Federal and law enforcement customers, and I currently teach a graduate level course on ethics, privacy, and policy at George Mason University for identity analysis.

The purpose of my testimony today is to provide the committee with an overview of the identity tech industry, our perspective on privacy and policy, and the status of the efficacy of facial recognition technology.

IBIA is the leading international trade group representing the identity tech industry. Our mission is to advance the adoption, responsible use of this technology for managing identity—human identity to enhance security, privacy, productivity, and convenience.

We have 27 member companies serving customers in the public and private sectors. The use cases of our customers include everything from law enforcement, security, national defense, finance, and health care, and many others.

Members of IBIA believe these technologies should be used solely for legal, ethical, and nondiscriminatory purposes. We are committed to the highest standards of system integrity and database security in order to deter identity theft, protect personal privacy, and ensure equal rights under the law.

The industry believes in transparency and openness with these systems. We support and encourage best practices to ensure privacy and ethical use. We believe it should be fielded with appropriate privacy policies that cover how the data are processed, stored, and used.

Let me say a couple of words about policy. IBIA sees many areas of shared consensus across this community where we can work together: Number one, we do not support the use of facial recognition in tracking or profiling individuals based solely on age, gender, race, ethnicity, or religion, or any other violation of constitutionally protected rights to free speech and assembly. Number two, we support a clear delineation on how data are used and who has access. We do not support a violation of statutes related to the use of data. Number three, Federal and State audits of these facial recognition systems are reasonable. Number four, there are existing policies and regulations in place. They should be reexamined and strengthened where necessary after a debate among all the stakeholders. And, number five, industry should have a limited access to real-world data for testing purposes.

Let me talk a little bit about what IBIA has done in this privacy debate. We participated in the NTIA multistakeholder process to develop and publish general guidelines. The output of that was the privacy best practices recommendation for commercial facial recognition use. We also are a member of the Future of Privacy Forum for at least 2 years.

Let me talk a little bit about the value of biometrics. This is a valuable national security tool and for law enforcement. According to a 2015 document published by the American Association of Motor Vehicles, John Robert Jones was convicted in 1974 of murdering a fellow soldier at Fort Dix, New Jersey. After 3 years in prison, Jones escaped and was on the run for more than 37 years under an assumed identity. He was listed as one of the Army's top 15 most wanted fugitives. The U.S. Marshals office submitted a photograph of Jones for comparison in the Florida DMV's facial recognition system. A match with an image on a driver's license that Jones had fraudulently acquired in 1981 was returned. Jones was subsequently apprehended, and his fingerprints confirmed he was indeed the wanted fugitive. These are valuable tools to produce leads and to capture known suspects.

A few words on accuracy. The accuracy of automated facial recognition technology has steadily improved over the past 15 years. For high-performing algorithms, error rates can be as low as 1 percent. So this means that, in most cases, they can match 99 percent of the time.

However, matching accuracy is highly dependent on image quality, image gallery quality, and the proprietary algorithm in use. The human element in training cannot be understated. Professionally trained humans are responsible for deciding to take action on a face match. Facial recognition is an investigative tool.

And, finally, race, ethnicity, gender, and age are not generally considered or factored into the mathematics of a facial recognition algorithm. Algorithms are developed to be as accurate as possible using mathematical vector sets, such as the number of pixels between the eyes. However, when dealing with homogeneous data sets of faces, there have been instances and test results where certain technologies' effectiveness has varied.

I thank you for this opportunity to testify today, and I look forward to your questions.

[Prepared statement of Mr. Hutchinson follows:]

WRITTEN STATEMENT

OF

JAMES BENJAMIN HUTCHINSON

TESTIMONY ON BEHALF OF THE INTERNATIONAL BIOMETRICS + IDENTITY ASSOCIATION (IBIA)

BEFORE THE

COMMITTEE ON OVERSIGHT & GOVERNMENT REFORM UNITED STATES HOUSE OF REPRESENTATIVES

LAW ENFORCEMENT'S USE OF FACIAL RECOGNITION TECHNOLOGY

PRESENTED

22 MARCH 2017

Introduction

Good morning Chairman Chaffetz, Ranking Member Cummings, Committee Members, and other distinguished guests. Thank you for inviting me to testify today. My name is Benji Hutchinson. I appear before you on behalf of the International Biometrics + Identity Association, more commonly known as IBIA. I am an employee of NEC Corporation of America. NEC Corporation of America is a member company of IBIA. I am appearing here in my personal capacity at the request of IBIA.

I have 13 years of experience in the biometrics, forensics, and identity technology industry. I have supported a wide range of customers throughout my career, largely federal national security agencies but also some law enforcement. I have held top secret security clearances and I currently teach a graduate level course on the ethics, privacy, policy, and law of identity analysis at George Mason University. Also, I chair the IBIA's Advances in Biometric Technology Working Group.

The purpose of my testimony today is to provide the committee with an overview of the identity technology industry, an understanding of biometrics and facial recognition technology, and the industry perspective on privacy.

Overview of IBIA and the Identity Industry

IBIA is the leading international trade group representing the identification technology industry. The association recognizes the vital role identity plays in a globally connected world. The mission of IBIA is to advance the adoption and responsible use of technologies for managing human identity to enhance security, privacy, productivity, and convenience for individuals, organizations, and governments. To effectively carry out this mission, IBIA focuses on three core activities: advocacy, connections, and education. IBIA brings broad industry stakeholders into a single organization to provide essential support for access to decision makers, inform members with industry reports, and establish a platform for debate on public policy and legislation regarding identity technology.

The biometrics and identity industry is a multi-billion dollar international industry with diverse offerings. Identity products include biometric software and hardware solutions for fingerprint, palm, iris, DNA, voice, and of course facial recognition solutions. Physical identity solutions include secure credentials such as passports

and common access smart cards. Our industry also offers professional services and subject matter expertise for customers with requirements to positively identify individuals for various reasons.

Member companies of IBIA serve various government agencies at the federal, state, and local levels. Our members also serve private sector clients. The missions and operations that IBIA supports include law enforcement, defense and counter terrorism, border management and travel security, education, finance, gaming, health care, cybersecurity, human resources, elections, physical access, and benefits distribution. We have 27 national and international member companies from across the identity technology industry. IBIA membership consists of large, established companies, mid-size, and new, small companies that have recently entered the market.

Basics of Biometrics

Biometrics are unique physical or behavioral characteristics which can be used to identify individuals. Biometric technologies capture, process and measure these characteristics electronically and compare them against existing records to create a highly accurate identity management capability. As previously mentioned, common physical biometric indicators in use today include fingerprints, faces, irises, voices, and DNA, among many others.

Biometrics have been around for over 100 years in various forms around the world for various use cases. In the U.S., the techniques of measuring fingerprints, latent fingerprints, and palm prints grew in popularity among the law enforcement community in the early 20th century. The modern digital version of biometrics in use today by law enforcement or national security professionals developed about 45 years ago. The technology has progressed rapidly in the past 16 years, largely due to heavy investment in research and development after the tragic terrorist attacks of 9/11.

Basics of Facial Recognition

1. **How does it work?** Facial recognition technology uses the layout of facial features and their distances from one another for identification against a "gallery" of faces with similar characteristics. These characteristics can be extracted and measured from either a still or video images. Using statistics,

facial recognition algorithms can measure the differences between the face being searched and the enrolled faces in a gallery. The smaller the difference, the more likely those faces match. Facial recognition technology is primarily used for anonymously characterizing faces, verification (1:1) searching known faces, and identification (1:N) searching unknown faces. (International Biometrics + Identity Association n.d.)

2. **What is a facial recognition algorithm?** Facial recognition algorithms are computer instructions that generally perform three functions: image processing, feature extraction, and matching. Image processing could include enhancing the quality of an image against a predetermined standard. Feature extraction is the process of locating points of interest or features in a digital face image that are relevant for matching. These features are then extracted, and a mathematical representation of the image is generated. Matching is the process of comparing multiple facial representations. The result of the matching process is a similarity score, which is then compared with the threshold value to determine a match or no-match decision by a human. (American Association of Motor Vehicle Administrators, Driver Standing Committee & Law Enforcement Standing Committee, Facial Recognition Working Group 2015)
3. **How accurate is the technology?** The accuracy of automated facial recognition technology has steadily improved over the past 15 years. For high performing facial algorithms, error rates can be as low as 1%. This means algorithms can match faces accurately around 99% of the time. However, it is important to note that matching accuracy is highly dependent on the quality of a face image, the quality and composition of the face images in a gallery, and the proprietary algorithm used to search and match. In 2014, the National Institute for Standards and Technology (NIST) found that the error rates continued to decline and algorithms had improved at identifying individuals from still photo images of poor quality or captured under low light (National Institute of Standards and Technology 2014) and (Government Accountability Office 2015). More recently in 2017 in a study on facial images from video, NIST found that with small galleries of 480 faces, the proportion of searches that do not yield the correct identity at rank 1 ranges from below 1% to above 40%. (National Institute of Standards and Technology n.d., 8). A final word on accuracy, the algorithmic facial

recognition process out performs human operators in terms of speed and accuracy when initially searching through large amounts of data. The final match decision, particularly for law enforcement applications, from search results is made by a human through their visual examination of ranked candidates returned by the automated search. Training of human examiners for this process is critical. Professionally trained humans are responsible for deciding to take action on a face match. In these applications, you can think of automated facial recognition as an "investigative tool" that returns several match candidates of interest that are then further investigated by a trained professional examiner. Similarly, in border security applications such as real time surveillance, the algorithms can be tuned to match only top candidates who surpass a certain score threshold, which would trigger a real time response. Even in these circumstances, trained professional examiners are responsible for taking action on any matches.

4. **How effective is facial recognition technology at dealing with race, ethnicity, gender, and certain age groups?** Race, sex, and age are not generally considered or factored into the mathematics of a facial recognition algorithm. These aspects are largely biographic and contextual data descriptors. Algorithms are developed to be as accurate as possible using mathematical feature sets such as the number of pixels between the eyes. It is important to note that it is in the best interest of our industry to develop highly accurate algorithms that do not consider such aspects at the algorithm level. However, when dealing with homogenous data sets of faces, there have been instances where the technology's effectiveness has varied with ethnicity, race, gender, and certain extreme age groups. Faces change over time. A baby does not have the same face at age 18 nor does that person have the same facial structure at age 70. Once a match is made, the human examiner must look at images analytically, not holistically. This approach helps to diffuse the possibility of human error because examiners look for analytical attributes that distinguish a face (e.g. moles, nose, nostrils). Facial recognition is a photographic comparison technique similar to other types of comparison in the field of forensic science.
5. **Would vendors allow customers access to source code for tuning?** As a general practice, the majority of facial recognition vendors would never allow customer access to the facial recognition algorithm source code as this

is considered proprietary information. If this occurred, it would be a rare exception. Vendors would never allow access to source code for tweaking or tuning an algorithm. This practice would open up technology companies to liability, void warranties, and undermine technology performance and credibility. Such a practice could ultimately destroy our business. Nevertheless, biometric software applications do allow users to tune search parameters. For example, operators can configure a system to return match results with candidates above or below a certain score threshold. Such parameters are common among all biometrics modalities and systems including fingerprint systems.

6. **How is the technology tested by industry?** Each vendor tests their algorithms with their own internal methodologies based on best practices developed by academia and industry research and development; and then outlined by the American National Standards Institute (ANSI), the International Standards Organization (ISO), and the National Institute of Standards and Technology (NIST). In addition, many members of IBIA submit facial algorithms to NIST for testing that is consistent, truly transparent to all, and according to a common methodology. The testing methodologies used by NIST to assess the efficacy of facial recognition algorithms are extensive and sophisticated.

The Value of Biometrics and Facial Recognition

Biometrics and facial recognition are effective tools to promote lower crime rates, enhance public safety, and prevent terrorism. During the wars of Iraq and Afghanistan, biometric and identity technologies matured rapidly and saved thousands of American lives on the battlefield. U.S. military forces employed (and still use today) these technologies in tactical and strategic forensic investigations, to pursue perpetrators of improvised explosive devices, and to defeat terrorist networks. Often times, enemy combatants did not wear military uniforms and they disappeared into crowds. Biometrics were critical tools in countering this threat. In the law enforcement arena, these tools have also been used countless times as an investigative tool to solve or prevent crimes. Here is just one example:

"John Robert Jones was convicted in 1974 of murdering a fellow soldier at Fort Dix, New Jersey. After three years in prison, Jones escaped and was on the run for more

than 37 years under an assumed identity. He was listed as one of the Army's top 15 most wanted fugitives. The U.S. Marshall's Office submitted a photograph of Jones for comparison in the Florida DMV's FR system. A match with an image on a driver's license that Jones had fraudulently acquired in 1981 was returned. Jones was subsequently apprehended, and his fingerprints confirmed he was indeed the wanted fugitive (American Association of Motor Vehicle Administrators, Driver Standing Committee & Law Enforcement Standing Committee, Facial Recognition Working Group 2015)."

Facial recognition is the enabling technology for deterring secure document issuance fraud. It is used by the majority of States and by the Department of State to ensure that an individual is issued only one unique document, driver's license, passport or a visa.

Facial Recognition is One of Many Biometrics Tools

These technologies are investigative tools for law enforcement agencies. They are based on statistics and are not absolute. None of the technologies represented by the IBIA will ever yield a 100% match by themselves. When an image is searched against a database of images, these technologies generate candidate lists, which represent investigative leads. Human operators must always review the results and take action on possible matches. Our customers often refer to our technology as investigative tools for generating leads. Face recognition is no different from other technologies used by law enforcement, such as voice, fingerprint or iris biometrics. Training is very important. We do support the continual education of how to effectively and responsibly use these tools. We also support the continued development of best practices and more standards on facial comparison.

IBIA Position on Ethics and Privacy

The members of IBIA believe that identification technologies should be used solely for legal, ethical, and non-discriminatory purposes. We are committed to the highest standards of systems integrity and database security in order to deter identity theft, protect personal privacy, and ensure equal rights under the law in all identification solutions.

The industry believes in and supports transparency and openness as it pertains to the capabilities of biometrics and identity technologies. We support and encourage

best practices to ensure privacy and ethical use of the technology. We believe the technology should be fielded with appropriate privacy policies in place that cover how the data are used, who has access, data sharing, data security, and data redress. Of course this functionality should be subject to applicable laws and policies of the U.S. federal government or the appropriate state.

IBIA Contribution to the Privacy Debate

According to IBIA's Privacy Best Practice Recommendations for Commercial Biometric Use, our primary privacy policy is that biometric data should be treated as personally identifiable information (PII) and, as such, all biometric data should be protected.

Over the years, IBIA has participated in, and will continue to participate in, discussions surrounding privacy and the responsible, ethical use of biometric technology. Specific examples of recent and past IBIA efforts to engage in the privacy debate are listed below:

a. **NTIA General Framework for Privacy** - IBIA Participated in the Department of Commerce, National Telecommunications and Information Administration (NTIA), Multi-Stakeholder Process to develop and publish a general framework for the commercial use of facial recognition titled the "Privacy Best Practice Recommendations for Commercial Facial Recognition Use."
b. **Annual 'connect:ID' Conference** – We co-sponsor this annual event that brings together government, academia, industry, privacy and policy experts all for the express purpose of discussing not only the latest trends in the technology, but also best ways to test, deploy, and enhance the technology in support of our customers and their missions. We also host specific panels on the ethical use of automated identity data as a social good.
c. **Active Member of the Future of Privacy Forum** – IBIA is an active member of the Future of Privacy Forum and has been for 2 years. We have a strong, collaborative relationship. Together, we work to co-develop papers on privacy issues, biometrics and identity technology, and education efforts.

d. **Participation in Public Discourse and Debate** – We accepted the Committee's invitation to participate in today's panel because we felt it was important to appear and provide an industry perspective.

We welcome the opportunity to have a constructive dialogue and collaborate with members of this panel and the broader identity technology community. As in any national or public debate, we may have disagreements with the logic and findings of particular groups, however, we remain committed to a continued dialogue. We encourage members of this public debate to not over emphasize or overstate the potential negative impacts of biometrics technology. As with any new technology or tool, misperceptions and misunderstandings are common. IBIA believes the benefits of identity technology far outweigh the negatives. Part of IBIA's charter is to continually educate the public on this technology.

In Closing

We thank the Committee for the opportunity to testify today. IBIA looks forward to continuing this dialogue with the members of this Committee and the members of this panel. We hope this testimony has helped the committee to better understand the technology of facial recognition and the perspective of the industry who develops it. We believe the ethics and privacy of biometrics and identity technology are important issues that will continually evolve over time. As an industry group, we look forward to participating in that debate by providing subject matter expertise on biometric and identity technology. Thank you very much.

Works Cited

American Association of Motor Vehicle Administrators, Driver Standing Committee & Law Enforcement Standing Committee, Facial Recognition Working Group. 2015. "Facial Recognition Program Best Pracitces." Best Practices, 28-29.

American Association of Motor Vehicle Administrators, Driver Standing Committee & Law Enforcement Standing Committee, Facial Recognition Working Group. 2015. "Facial Recognition Program Best Practices." Best Practices, 48.

Government Accountability Office. 2015. "Facial Recognition Technology, Commercial Uses, Privacy Issues, and Applicable Federal Laws." GAO, 5.

IBIA. n.d. *Face Biometrics.* https://www.ibia.org/biometrics-and-identity/biometric-technologies/face.

International Biometrics + Identity Association. n.d. *IBIA Face Biometrics.* https://www.ibia.org/biometrics-and-identity/biometric-technologies/face.

National Institute of Standards and Technology. n.d. *Face in Video Evaluation (FIVE), Face Recognition of Non-Cooperative Subjects.* NISTIR, NIST, Gaithersburg: NIST.

National Institute of Standards and Technology. 2014. *Face Recognition Vendor Test (FRVT): Performance of Face Identification Algorithms.* NIST, Gaithersburg: NIST.

Chairman CHAFFETZ. Thank you.

Ms. Lynch, you're now recognized for 5 minutes.

STATEMENT OF JENNIFER LYNCH

Ms. LYNCH. Chairman Chaffetz, Ranking Member Cummings, and members of the committee, thank you very much for the invitation to testify today.

Since my 2012 testimony on face recognition before the Senate Subcommittee on Privacy, Technology, and the Law, face recognition technologies have advanced significantly. Now, law enforcement officers can use mobile devices to capture face-recognition-ready photographs of people they stop on the street. Surveillance cameras boast real-time tracking and face scanning and identification capabilities, and the FBI has access to hundreds of millions of face recognition images of law-abiding Americans.

However, the adoption of face recognition technologies like these has occurred without meaningful oversight, without proper accuracy testing, and without legal protections to prevent their misuse. This has led to the development of unproven systems that will impinge on constitutional rights and disproportionately impact people of color.

The FBI's Interstate Photo System and FACE Services Unit exemplify these problems. The minimal testing conducted by the Bureau showed the IPS was incapable of accurate identification at least 15 percent of the time. This has real-world consequences. An inaccurate system will implicate people for crimes they didn't commit, and it will shift the burden onto innocent defendants to show they are not who the system says they are.

This threat will disproportionately impact people of color. Face recognition misidentifies African Americans and ethnic minorities at higher rates than whites. Because mugshot databases include a disproportionate number of African Americans, Latinos, and immigrants, people of color will likely shoulder exponentially more of the burden of the IPS' inaccuracies than whites.

Despite these known challenges, FBI has for years failed to be transparent about its use of face recognition. It took 7 years to update its Privacy Impact Assessment for the IPS and didn't release a new PIA until a year after the system was fully operational.

And the public had no idea how many images were accessible to its FACE Services Unit until last year's GAO report revealed the Bureau could access nearly 412 million images, most of which were taken for noncriminal reasons, like obtaining a driver's license or a passport.

Without transparency, accountability, and proper security protocols in place, face recognition systems may be vulnerable to security breach and misuse. This has already occurred in other contexts. For example, in 2010, ICE enlisted local police officers to use license plate readers to gather information on gun show customers. In 2015, hackers breached the Office of Personnel Management systems and stole sensitive data, including biometric data, on more than 25 million people. And in 2015, the Baltimore Police may have used face recognition and social media to identify and arrest people in the protests following Freddie Gray's death.

Americans should not be forced to submit to criminal face recognition searches merely because they want to drive a car. They shouldn't have to worry their data will be misused by unethical government officials or stolen in a security breach. And they shouldn't have to fear that their every move will be tracked if the network of surveillance cameras that already blanket many cities are linked to face recognition.

But without meaningful legal protections, this is where we may be headed. Without laws in place, it could be relatively easy for the government to amass databases of images of all Americans and use those databases to identify and track people in real time as they go about their daily lives.

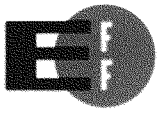
As this committee noted in its excellent 2016 report on law enforcement use of cell-site simulators, advances in emerging surveillance technologies, like face recognition, require careful evaluation to ensure their use is consistent with the protections afforded under the First and Fourth Amendments.

And just as with cell-site simulators, transparency and accountability are critical to ensuring that face recognition's use not only comports with constitutional protections but also preserves democratic values.

Justice Alito noted in his concurring opinion in United States v. Jones that, in circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. Just as this committee found with cell-site simulators, the use of face recognition must be limited. Specifically, law enforcement should be required to get a warrant before accessing noncriminal face recognition databases and before conducting real-time tracking and identification.

I urge this committee to introduce legislation to do just that. Thank you once again for the invitation to testify. I'm happy to respond to questions.

[Prepared statement of Ms. Lynch follows:]



ELECTRONIC FRONTIER FOUNDATION

United States House Committee on
Oversight and Government Reform

Hearing on Law Enforcement's Use of Facial Recognition Technology

Written Testimony of
Jennifer Lynch
Senior Staff Attorney
Electronic Frontier Foundation (EFF)

March 22, 2017

For further information, please contact Jennifer Lynch at
jlynch@eff.org *or* 415.436.9333x136

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee:

Thank you very much for the opportunity to discuss facial recognition technology. My name is Jennifer Lynch, and I am a senior staff attorney with the Electronic Frontier Foundation (EFF), a non-profit, member-supported, public-interest organization that works to protect privacy and civil liberties in new technologies.[1]

I. Introduction

Since my 2012 testimony on face recognition before the Senate Subcommittee on Privacy, Technology, and the Law,[2] face recognition technology has advanced significantly. Now, law enforcement officers can use mobile devices to capture face recognition-ready photographs of people they stop on the street; surveillance cameras boast real-time face scanning and identification capabilities; and the FBI has access to hundreds of millions of face recognition images of law-abiding Americans.

However, the adoption of face recognition technologies like these has occurred without meaningful oversight, without proper accuracy testing of the systems as they are actually used in the field, and without the enactment of legal protections to prevent their misuse.

This has led to the development of unproven, inaccurate systems that will impinge on constitutional rights and disproportionately impact people of color.

The FBI's Interstate Photo System and FACE Services Unit exemplify these problems. The minimal testing conducted by the Bureau showed the IPS was incapable of accurate identification at least 15% of the time. This has real-world impact; an inaccurate system will implicate people for crimes they didn't commit, forcing them to try to prove their innocence and shifting the traditional burden of proof away from the government.

This threat will likely disproportionately impact people of color. Face recognition misidentifies African Americans and ethnic minorities, young people, and women at

---

[1] Founded in 1990, EFF represents the interests of tens of thousands of dues-paying members and the public in both court cases and broader policy debates surrounding the application of law in the digital age. EFF is particularly concerned with protecting privacy at a time when technological advances have resulted in increased surveillance by the government and actively encourages and challenges government and the courts to support privacy and safeguard individual autonomy as emerging technologies become prevalent in society.

[2] *See Testimony of Jennifer Lynch to the Senate Committee on the Judiciary Subcommittee on Privacy, Technology, and the Law* (July 18, 2012) *available at* https://www.eff.org/files/filenode/jenniferlynch_eff-senate-testimony-face_recognition.pdf.

higher rates than whites, older people, and men, respectively.[3] Due to years of well-documented, racially-biased police practices, all criminal databases—including mug shot databases—include a disproportionate number of African Americans, Latinos, and immigrants.[4] These two facts mean people of color will likely shoulder exponentially more of the burden of the Interstate Photo System's inaccuracies than whites.

Despite these known challenges, FBI has for years also failed to be transparent about its use of face recognition technology. It took seven years to update its Privacy Impact Assessment for the IPS and didn't release one until a year after its system was fully operational. And the public had no idea how many images were accessible to its FACE Services Unit until last year's scathing Government Accountability Office report revealed the Bureau could access nearly 412 million images—most of which were taken for non-criminal reasons like obtaining a driver license or a passport.

Without transparency, accountability, and proper security protocols in place, face recognition systems—like many other searchable databases of information available to law enforcement—may be subject to misuse. This misuse has already occurred in other contexts. For example, in 2010, Immigration and Customs Enforcement enlisted local police officers to use license plate readers to gather information about gun-show customers.[5] In Florida in 2011, more than 100 officers accessed driver and vehicle information for a female Florida state trooper after she pulled over a Miami police officer for speeding.[6] And a state audit that same year of law enforcement access to driver information in Minnesota revealed "half of all law-enforcement personnel in Minnesota

---

[3] *See* B. F. Klare, M. J. Burge, J. C. Klontz, R. W. Vorder Bruegge and A. K. Jain, "Face Recognition Performance: Role of Demographic Information," in,*IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1789-1801, (Dec. 2012). http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6327355&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Ficp.jsp%3Farnumber%3D6327355. *See also* Clare Garvie & Jonathan Frankle, "Facial-Recognition Software Might Have a Racial Bias Problem," *The Atlantic* (Apr. 7, 2016) http://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/.

[4] *See* NAACP, Criminal Justice Fact Sheet (2009) *available at* https://donate.naacp.org/pages/criminal-justice-fact-sheet.

[5] Devlin Barrett, *Gun-Show Customers' License Plates Come under Scrutiny*, Wall St. J. (Oct. 2, 2016), http://www.wsj.com/articles/gun-show-customers-license-plates-come-under-scrutiny-1475451302.

[6] Dave Elias, *Deputy fired for misusing driver's license database*, NBC2 (April 24, 2014) http://www.nbc-2.com/story/25334275/deputy-fired-for-improperly-accessing-info-about-governor-nbc2-anchors-others.

had misused driving records."[7]

Americans should not be forced to submit to criminal face recognition searches merely because they want to drive a car. They shouldn't have to worry their data will be misused by unethical government officials with unchecked access to face recognition databases. And they shouldn't have to fear that their every move will be tracked if face recognition is linked to the networks of surveillance cameras that blanket many cities.

But without meaningful legal protections, this is where we may be headed. Without laws in place, it could be relatively easy for the government and private companies to amass databases of images of all Americans and use those databases to identify and track people in real time as they move from place to place throughout their daily lives. As researchers at Georgetown discovered last year, 1 out of 2 Americans is already in a face recognition database accessible to law enforcement.[8]

As this Committee noted in its excellent 2016 report on law enforcement use of cell-site simulators, "advances in emerging surveillance technologies" like face recognition "require careful evaluation to ensure their use is consistent with the protections afforded under the First and Fourth Amendments to the U.S. Constitution."[9] And, just as with cell-site simulators, transparency and accountability are critical to ensuring that face recognition's use not only comports with Constitutional protections but also preserves democratic values.

Justice Alito noted in his concurring opinion in *United States v. Jones* that, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."[10] Just as this Committee found with cell-site simulators, the use of face recognition must be limited. I urge the Committee to introduce legislation to do just that.

---

[7] Chris Francescani, *License to Spy,* Medium (Dec. 1, 2014), https://medium.com/backchannel/the-drive-to-spy-80c4f85b4335.

[8] Clare Garvie, et al., *The Perpetual Line-Up*, Georgetown Law Center on Privacy & Technology (Oct. 18, 2016) https://www.perpetuallineup.org/jurisdiction/florida.

[9] *Law Enforcement Use of Cell Site Simulation Technologies: Privacy Concerns and Recommendations*, House Committee on Oversight & Government Reform (Dec. 19, 2016) *available at* https://oversight.house.gov/wp-content/uploads/2016/12/THE-FINAL-bipartisan-cell-site-simulator-report.pdf.

[10] 565 U.S. 400, 429 (2012) (Alito, J., concurring).

II. FBI's Next Generation Identification Database and the Interstate Photo System

The FBI's Next Generation Identification system (NGI) is a massive biometric database that includes fingerprints, iris scans, and palm prints collected from individuals not just during arrests, but also from millions of Americans and others for non-criminal reasons like background checks, state licensing requirements, and immigration, The Interstate Photo System (IPS) is the part of NGI that contains images like mug shots and non-criminal photographs that are searchable through face recognition. Each of these biometric identifiers is linked to personal, biographic, and identifying information, and, where possible, each file includes multiple biometric identifiers. FBI has designed NGI to be able to expand in the future as needed to include "emerging biometrics," such as footprint and hand geometry, gait recognition, and others.[11]

NGI incorporates both criminal and civil records. NGI's criminal file includes records on people arrested at the local, state, and federal level as well as biometric data taken from crime scenes and data on missing and unidentified persons. NGI's civil repository stores biometric and biographic data collected from members of the military and those applying for immigration benefits. It also includes biometric data collected as part of a background check or state licensing requirement for many types of jobs, including licensing to be a dentist, accountant, teacher, geologist, realtor, lawyer or even an optometrist. Since 1953, all jobs with the federal government have also required a fingerprint check, no matter the salary range or level of responsibility.[12]

---

[11] FBI, *Next Generation Identification*, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi; FBI, *Biometric Center of Excellence*, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-center-of-excellence/modalities.

[12] *See, e.g.,* Dental Board of Cal., *Fingerprint Requirement for License Renewal* (2016) *available at* http://www.dbc.ca.gov/licensees/fingerprint_faq.shtml#q1; Texas State Board of Public Accountancy, *New Fingerprinting Process for CPA Exam Applicants* (August 1, 2014) https://www.tsbpa.texas.gov/info/2014072801.html; Wisc. Dept of Public Instruction, *Completing the Fingerprint Requirement* (August 1, 2013) http://dpi.wi.gov/tepdl/licensing/fingerprint; *See* Cal. Dept. of Consumer Affairs Bd for Professional Engineers, Land Surveyors, and Geologists, *Fingerprinting FAQ's* (2012) http://www.bpelsg.ca.gov/applicants/fingerprinting_faqs.shtml; State of New Jersey Dept. of Banking & Insurance, *Real Estate License Candidate Fingerprinting* (February 1, 2015) http://www.state.nj.us/dobi/division_rec/licensing/fingerprint.html; The State Bar of Cal., *Moral Character Determination Instructions* (2016) https://www.calbarxap.com/applications/calbar/info/moral_character.html#fingerprints; Cal. Dept. of Consumer Affairs Bd of Optometry,

As of February 2017, NGI included nearly 73 million records in the criminal repository and over 53 million records in the civil repository.[13] By December 2015, it also already contained nearly 30 million civil and criminal photographs searchable through face recognition.[14]

The states have been very involved in the development of the NGI database. NGI includes more than 20 million civil and criminal images received directly from at least six states, including California, Louisiana, Michigan, New York, Texas, and Virginia. And it appears five additional states—Florida, Maryland, Maine, New Mexico, and Arkansas—can send search requests directly to the NGI database. As of December 2015, FBI was working with eight more states to grant them access to NGI, and an additional 24 states were also interested.[15]

In 2015, FBI announced that for the first time it would link almost all of the non-criminal data in NGI with criminal data as a "single identity record."[16] This means that now, if a person submits fingerprints as part of their job search, those prints will be searched continuously along with the criminal prints thousands of times a day[17] for any crime by more than 20,000 law enforcement agencies across the country and around the world.[18]

FBI has said—for now—that it is keeping non-criminal photographs in the IPS separate

---

Fingerprint Requirement for License Renewal (June 21, 2010) http://www.optometry.ca.gov/faqs/fingerprint.shtml#q1.

[13] *See* FBI, *Next Generation Identification (NGI) Monthly Fact Sheet* (February 2017) *available at* https://www.fbi.gov/file-repository/ngi-monthly-fact-sheet/view (hereinafter "February 2017 NGI Monthly Fact Sheet").

[14] Government Accountability Office, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, 46, GAO-16-267 (May 2016) http://www.gao.gov/assets/680/677098.pdf (hereinafter "GAO Report").

[15] GAO Report at 13. The Report does not list these remaining states.

[16] FBI, *Next Generation Identification (NGI)—Retention and Searching of Noncriminal Justice Fingerprint Submissions* (Feb. 20, 2015) https://www.fbi.gov/foia/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions.

[17] *See* Adam Vrankulj, *NGI: A closer look at the FBI's billion-dollar biometric program* (November 4, 2013) *available at* http://www.biometricupdate.com/201311/ngi-a-closer-look-at-the-fbis-billion-dollar-biometric-program.

[18] *See* February 2017 NGI Monthly Fact Sheet.

from criminal photographs.[19] However, if a person is ever arrested for any crime—even for something as minor as blocking a street as part of a First Amendment-protected protest—their non-criminal photographs will be combined with their criminal record and will become fair game for the same face recognition searches associated with any criminal investigation.[20] As of December 2015, over eight million civil records were also included in the criminal repository.[21]

III. FBI Access to External Face Recognition Databases

The public did not begin to learn about FBI's ability to access external face recognition databases until the Bureau issued a Privacy Impact Assessment (PIA) for its Facial Analysis, Comparison, and Evaluation (FACE) Services Unit in May 2015. However, the full scope of that access was not revealed until the Government Accountability Office (GAO) issued its scathing report on FBI use of face recognition over a year later.

The GAO Report disclosed for the first time that FBI had access to over 400 million face recognition images—hundreds of millions more than journalists and privacy advocates had been able to estimate before that. According to the GAO Report, the FACE Services unit not only has access to FBI's Next Generation Identification (NGI) face recognition database of nearly 30 million civil and criminal mug shot photos, it also has access to the State Department's Visa and Passport databases, the Defense Department's biometric database, and the drivers license databases of at least 16 states. Totaling 411.9 million images, this is an unprecedented number of photographs, and most of these were collected from Americans and foreigners under civil and not criminal circumstances.

Under agreements we have never seen between the FBI and its state and federal partners, the FBI may search these civil photos whenever it is trying to find a suspect in a crime. And FACE Services has been searching its external partner databases a lot; from August 2011 through December 2015, the FBI requested nearly 215,000 searches of external

---

[19] *See* Ernest J. Babcock, Senior Component Official for Privacy, FBI, *Privacy Impact Assessment for the Next Generation Identification (NGI) Interstate Photo System* (September 2015) *available at* https://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system.

[20] *See, e.g.*, AZ Rev. Stat. § 13-2906 (Obstructing a highway or other public thoroughfare; classification).

[21] *See* FBI, *Next Generation Identification (NGI) Monthly Fact Sheet* (December 2015) *available at* https://web.archive.org/web/20160331181001/https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/december-2015-ngi-fact-sheet.pdf (hereinafter "December 2015 NGI Monthly Fact Sheet"). The FBI's current Monthly Fact Sheet omits this information. *Compare* February 2017 NGI Monthly Fact Sheet.

partners' databases.[22] FACE Services also receives thousands of requests from those partners for its services; since the beginning of the current fiscal year, it received more than 28,000 requests for face recognition-related searches.[23]

IV. For Years, FBI Failed to Produce Basic Information about NGI and its Use of Face Recognition as Required by Federal Law

Despite going live with NGI in increments since at least 2008, FBI failed to release basic information about its system, including mandatory PIAs and a new System of Records Notice (SORN), that would have informed the public on what data the FBI has been collecting and how that data is being used and protected.[24]

In failing to issue timely PIAs for the Interstate Photo System and the work of the FBI's FACE Services Unit, as well as a SORN for the entire NGI system, FBI also failed to comply with key provisions of both the Privacy Act of 1974 and the E-Government Act of 2002.[25]

PIAs are an important check against the encroachment on privacy by the government. They allow the public to see how new programs and technology used by the government affect their privacy and assess whether the government has done enough to mitigate the privacy risks. As the DOJ's own guidelines on PIAs explain, "[t]he PIA also . . . helps promote trust between the public and the Department by increasing transparency of the Department's systems and missions."[26] The are also mandatory.[27]

PIAs should also be conducted during the development of any new system "with sufficient lead time to permit final Departmental approval and public website posting on

---

[22] GAO Report at 10.

[23] *See* February 2017 NGI Monthly Fact Sheet.

[24] EFF and other organizations called for years on FBI to release more information about NGI and how it impacts people's privacy. *See, e.g.*, *Testimony of Jennifer Lynch to the Senate Committee on the Judiciary Subcommittee on Privacy, Technology, and the Law* (July 18, 2012) *available at* https://www.eff.org/document/testimony-jennifer-lynch-senate-committee-judiciary-subcommittee-privacy-technology-and-law; Letter to Attorney General Holder re. Privacy Issues with FBI's Next Generation Identification Database (June 24, 2014) *available at* https://www.eff.org/document/letter-attorney-general-holder-re-privacy-issues-fbis-next-generation-identification.

[25] 5 U.S.C. § 552a; Public Law 107–347 (2002).

[26] OPCL DOJ, Privacy Impact Assessments Official Guidance, 3 (Rev. March 2012) *available at* https://www.justice.gov/opcl/docs/2012-doj-pia-manual.pdf.

[27] *Id.* (footnotes omitted).

or before the commencement of any system operation (including before any testing or piloting.)"[28]

Despite these requirements, FBI began developing one of NGI's most important capabilities—face recognition—by at least 2008, and it issued a PIA for the IPS that same year. However, it didn't update that PIA until late 2015—a full year after the entire Interstate Photo System was online and fully operational and as many as seven years after FBI first started incorporating face recognition-compatible photographs into NGI.[29] Before FBI issued the new PIA, it had already conducted over 100,000 searches of the database.[30]

FBI also failed to produce a System of Records Notice (SORN) for the NGI system until 2016.[31] The Privacy Act requires all federal agencies to produce a SORN for any system that collects and uses Americans' personal information.[32] Those SORNs must describe exactly what data is collected and how it is being used and protected. But for years FBI skirted the Privacy Act—instead of producing a new System of Records Notice (SORN) for NGI, it relied on an outdated SORN from 1999 describing its legacy IAFIS database[33]—a database that only included fingerprints and non-searchable photographs. Even FBI now admits that NGI contains nine "enhancements" that make it fundamentally different from the original IAFIS database that it replaces.[34]

The GAO Report specifically faulted FBI for amassing, using, and sharing its face recognition technologies without ever explaining the privacy implications of its actions to the public. As GAO noted, the whole point of a PIA is to give the public notice of the privacy implications of data collection programs and to ensure that privacy protections

---

[28] *Id.* at 4.

[29] FBI, *Privacy Impact Assessment for the Next Generation Identification (NGI) Interstate Photo System* (Sept. 2015) https://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system (hereinafter "2015 FBI Interstate Photo System PIA"); *see also* Tim Cushing, *FBI Rolls Out Biometric Database On Schedule, Accompanying Privacy Impact Assessment Still Nowhere To Be Found* (September 16, 2014) https://www.techdirt.com/articles/20140916/09090628533/fbi-rolls-out-biometric-database-schedule-accompanying-privacy-impact-assessment-still-nowhere-to-be-found.shtml.

[30] GAO Report at 49.

[31] 81 Fed. Reg. 27283 (May 5, 2016).

[32] 5 U.S.C. § 552a(e)(4).

[33] FBI, 64 FR 52343 (09-28-99) https://www.fbi.gov/foia/privacy-act/64-fr-52343.

[34] Proposed FBI NGI SORN.

are built into the system from the start. FBI failed to do this.

V. NGI is Inaccurate, Impinges on First and Fourth Amendment Rights, and Disproportionately Impacts People of Color

A. FBI Has Failed to Address the Problem of Face Recognition Inaccuracy

FBI has done little to ensure its face recognition search results (which the Bureau calls "investigative leads") do not implicate innocent people. According to the GAO report and FBI's responses to EFF's Freedom of Information Act requests, FBI has conducted only very limited testing to ensure the accuracy of NGI's face recognition capabilities. And it has not taken any steps to determine whether the face recognition systems of its external partners—states and other federal agencies—are sufficiently accurate to prevent innocent people from being identified as criminal suspects.

FBI admits its system is inaccurate, noting in its PIA for the Interstate Photo System that IPS "may not be sufficiently reliable to accurately locate other photos of the same identity, resulting in an increased percentage of misidentifications."[35] However, FBI has disclaimed responsibility for accuracy in its face recognition system, stating that "[t]he candidate list is an investigative lead not an identification."[36] Because the system is designed to provide a ranked list of candidates, FBI has stated NGI never actually makes a "positive identification," and "therefore, there is no false positive rate."[37] In fact, FBI only ensures that "the candidate will be returned in the top 50 candidates" 85 percent of the time "when the true candidate exists in the gallery."[38] It is unclear what happens when the "true candidate" does *not* exist in the gallery, however—does NGI still return possible matches? Could those people then be subject to criminal investigation for no other reason than that a computer thought their face was mathematically similar to a suspect's?

The GAO Report criticizes FBI's cavalier attitude regarding false positives, noting that "reporting a detection rate without reporting the accompanying false positive rate presents an incomplete view of the system's accuracy."[39] The Report also notes that

---

[35] 2015 FBI Interstate Photo System PIA.

[36] *See* Jennifer Lynch, *FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year*, and accompanying documents. The Bureau has also noted that because "this is an investigative search and caveats will be prevalent on the return detailing that the [non-FBI] agency is responsible for determining the identity of the subject, there should be NO legal issues." *Id.*

[37] *Id.*

[38] *Id.*

[39] GAO Report at 27.

FBI's stated detection rate may not represent operational reality because FBI only conducted testing on a limited subset of images and failed to conduct additional testing as the size of the database increased. FBI also has never tested to determine detection rates where the size of the responsive candidate pool is reduced to a number below 50.[40]

When false positives represent real people who may become suspects in a criminal investigation, the number of false positives a system generates is especially important.[41] But technical issues endemic to all facial recognition systems mean false positives will continue to be a common problem for the foreseeable future.

Face recognition technologies perform well when all the photographs are taken with similar lighting and shot from a frontal perspective (like a mug shot). However, when photographs that are compared to one another contain different lighting, shadows, different backgrounds, or different poses or expressions, the error rates can be significant.[42] Face recognition is also less accurate with large age discrepancies (for example, if people are compared against a photo taken of themselves when they were ten years younger).

Face recognition is also extremely challenging at low resolutions.[43] EFF learned through documents FBI released in response to our 2012 FOIA request that the median resolution of images submitted through an Interstate Photo System pilot program was "well-below" the recommended resolution of 3/4 of a megapixel (in comparison, newer iPhone cameras are capable of twelve megapixel resolution[44]).[45] Another FBI document released to EFF

---

[40] GAO Report at 26.

[41] Security researcher Bruce Schneier has noted that even a 90% accurate system "will sound a million false alarms for every real terrorist" and that it is "unlikely that terrorists will pose for crisp, clear photos." Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, 190 (2003).

[42] *See, e.g.*, P. Jonathon Phillips, et al., "An Introduction to the Good, the Bad, & the Ugly Face Recognition: Challenge Problem," *National Institute of Standards & Testing* (Dec. 2011), *available at* www.nist.gov/itl/iad/ig/upload/05771424.pdf (noting only 15% accuracy for face image pairs that are "difficult to match").

[43] *See, e.g.*, Min-Chun Yang, et al., Recognition at a Long Distance: Very Low Resolution Face Recognition and Hallucination, IEEE 2015 International Conference on Biometrics, 237-242 (May 2015).

[44] *See* Apple, *Compare iPhone Models* (2017) *available at* https://www.apple.com/iphone/compare/.

noted that because "the trend for the quality of data received by the customer is lower and lower quality, specific research and development plans for low quality submission accuracy improvement is highly desirable."

Finally, Face recognition performs worse overall as the size of the data set (the population of people you are checking against) increases, in part because so many people within a given population look similar to one another. At 30 million searchable photos so far, the FBI's face recognition system constitutes a very large data set.

Given all of these challenges, identifying an unknown face in a crowd using NGI's database of face images would still be particularly challenging.[46]

Using humans to perform the final suspect identification from a group of photos provided by the system does not solve these accuracy problems. Research has shown that, without specialized training, humans may be worse at identification than a computer algorithm. And that is especially true when the person is someone they don't already know or someone of a race or ethnicity different from their own.[47]

---

[45] *See* Jennifer Lynch, *FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year*, EFF (April 14, 2014) and accompanying documents at https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year.

[46] A 2009 New York University report concluded that, given these challenges, it is unlikely that face recognition systems with high accuracy rates under these conditions will become an "operational reality for the foreseeable future." Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, p. 3, N.Y.U. (April 2009) http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf. Recently, Russian developers announced that their system, called FindFace, could identify a person on the street with about 70% accuracy if that person had a social media profile. However, it is unclear at what resolution and distance the probe photos were taken and how many images of each person were available to compare the probe photos against (more photographs taken from different angles and under different lighting conditions could increase the probability of a match). *See, e.g.*, Ben Guarino, *Russia's new FindFace app identifies strangers in a crowd with 70 percent accuracy*, Wash. Post (May 18, 2016) https://www.washingtonpost.com/news/morning-mix/wp/2016/05/18/russias-new-findface-app-identifies-strangers-in-a-crowd-with-70-percent-accuracy/.

[47] *See* Clare Garvie, et al., *The Perpetual Line-Up*, Georgetown Law Center on Privacy & Technology, 49 (Oct. 18, 2016)(internal citations omitted).

B. The Scope of NGI and FBI's Use of Face Recognition Are Still Unclear

Although FBI finally produced a proposed SORN for NGI in Summer 2016, there is still a lot the public does not know about the system and FBI's plans for its future evolution. For example, a Request for Proposals FBI released in 2015 indicated the agency planned to allow law enforcement officers to use mobile devices to collect face recognition data out in the field and submit that data directly to NGI.[48] As we have seen with state and local agencies that have already begun using such devices, officers may use mobile biometric tools in ways that push the limits of and in some cases directly contradict constitutional law. For example, in San Diego, where officers from multiple agencies use mobile devices to photograph people right on the street and immediately upload those images to a shared face recognition database, officers have pressured citizens to consent to having their picture taken.[49] Regional law enforcement policy has also allowed collection based on First-Amendment protected activities like an "individual's political, religious, or social views, associations or activities" as long as that collection is limited to "instances directly related to criminal conduct or activity."[50]

From FBI's past publications related to NGI, including the Request for Proposals, the PIA for the Interstate Photo System, and the SORN for NGI, it is unclear whether FBI would retain the images collected with mobile devices in the NGI database. If it does, this would directly contradict 2012 congressional testimony where an FBI official said "[o]nly criminal mug shot photos are used to populate the national repository."[51] A photograph taken in the field before someone is arrested is not a "mug shot."

FBI may also decide to use NGI in other ways. A 2011 Memorandum of Understanding (MOU) between Hawaii and FBI shows that the government has considered "permit[ting] photo submissions independent of arrests."[52] It is not clear from the document, what

---

[48] *See* Jennifer Lynch, *FBI Plans to Populate its Massive Face Recognition Database with Photographs Taken in the Field*, EFF (Sept. 18, 2015) https://www.eff.org/deeplinks/2015/09/little-fanfare-fbi-ramps-biometrics-programs-yet-again-part-2.

[49] *See* Jennifer Lynch and David Maas, *San Diego Gets in Your Face With New Mobile Identification System*, EFF (Nov. 7, 2013) https://www.eff.org/deeplinks/2013/11/san-diego-gets-your-face-new-mobile-identification-system.

[50] *Id.*

[51] Jerome M. Pender, Deputy Assistant Director, Criminal Justice Information Services Division, FBI, *Statement Before the Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law* (July 18, 2012) https://www.fbi.gov/news/testimony/what-facial-recognition-technology-means-for-privacy-and-civil-liberties.

[52] *Hawaii Memorandum of Understanding (MOU) with FBI for Face Recognition Photos*

types of photos this could include. The Bureau also indicated in a 2010 presentation that it wants to use NGI to track people's movements to and from "critical events" like political rallies, to identify people in "public datasets," to "conduct[] automated surveillance at lookout locations," and to identify "unknown persons of interest" from photographs.[53] This suggests FBI wants to be able to search and identify people in photos of crowds and in pictures posted on social media sites—even if the people in those photos haven't been arrested for or suspected of a crime.

FBI's 2015 PIA for the Interstate Photo System and its proposed SORN leave open this possibility that FBI may plan to incorporate crowd or social media photos into NGI in the future. The PIA notes that NGI's "unsolved photo file" contains photographs of "unknown subjects," and the SORN notes the system includes "biometric data" that has been "retrieved from locations, property, or persons associated with criminal or national security investigations."[54] Because criminal investigations may occur in virtual as well as physical locations, this loophole seems to allow FBI to include images collected from security cameras, social media accounts, and other similar sources.

Finally, at some point in the future, FBI may also attempt to populate NGI with millions of other non-criminal photographs. The GAO Report notes FBI's FACE Services unit already has access to the IPS, the State Department's Visa and Passport databases, the Defense Department's biometric database, and the drivers license databases of at least 16 states.[55] However, the combined 412 million images in these databases may not even represent the full scope of FBI access to face recognition data today. When GAO's Report first went to press, it noted that FBI officials had stated the Bureau was in negotiations with 18 additional states to obtain access to their drivers license databases.[56] This information was kept out of later versions of the Report, so it is unclear where these negotiations stand today. The later version of the report also indicates Florida does not share its drivers license data with FBI, but Georgetown's recent report on law enforcement access to state face recognition databases contradicts this; Georgetown

---

(November 20, 2011) *available at* https://www.eff.org/document/hawaii-memorandum-understanding-mou-fbi-face-recognition-photos.

[53] *See* Richard W. Vorder Bruegge, *Facial Recognition and Identification Initiatives*, Federal Bureau of Investigation 5 (2010) *available at* https://www.eff.org/document/fbi-facial-recognition-initiatives-presentation-2010-biometrics-conference.

[54] Proposed FBI NGI SORN.

[55] GAO Report at 47-48.

[56] *Compare* map of states sharing data with FACE Services on page 51 of the GAO Report with map available in original version of Report, available here: https://www.eff.org/deeplinks/2016/06/fbi-can-search-400-million-face-recognition-photos.

found FBI field offices in Florida can search all drivers license and ID photos in the state.[57]

C. Face Recognition Uniquely Impacts Civil Liberties

These uses of NGI would clearly impact Fourth Amendment rights and First Amendment-protected activities and would chill speech. They could also violate a key provision of the Privacy Act designed to prevent data collection on First Amendment protected activities.[58] The addition of crowd and security camera photographs and DMV photographs into NGI would mean that anyone could end up in the database without their knowledge—even if they're not suspected of a crime—by just happening to be in the wrong place at the wrong time, by fitting a stereotype that some in society have decided is a threat, or by, for example, engaging in "suspect" activities such as political protest in public spaces rife with cameras. Given FBI's history of misuse of data gathered on people during former FBI director J. Edgar Hoover's tenure[59] and during the years following September 11, 2001,[60]—data collection and misuse based on religious beliefs, race, ethnicity, and political leanings—Americans have good reason to be concerned about expanding government face recognition databases.

Face recognition technology, like other biometrics programs that collect, store, share, and combine sensitive and unique data poses critical threats to privacy and civil liberties. Biometrics in general are immutable, readily accessible, individuating and can be highly prejudicial. Face recognition, though, takes the risks inherent in other biometrics to a new level because individuals cannot take precautions to prevent the collection of their image. Face recognition allows for covert, remote, and mass capture and identification of

---

[57] Clare Garvie, et al., *The Perpetual Line-Up*, Georgetown Law Center on Privacy & Technology (Oct. 18, 2016) https://www.perpetuallineup.org/jurisdiction/florida.

[58] *See* 5 U.S.C. 552a(e)(7) (forbidding agencies from maintaining "records describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity").

[59] *See generally* Tim Weiner, *Enemies: A History of the FBI* (2012).

[60] *See, e.g.*, DOJ, Office of Inspector General (OIG), *A Review of the Federal Bureau of Investigation's Use of National Security Letters, Special Report* (March 2007); DOJ, OIG, *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006, Special Report*, (March 2008); DOJ, OIG, *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records* (January 2010).

images[61]—and the photos that may end up in a database could include not just a person's face but also how she is dressed and possibly whom she is with.

Face recognition and the accumulation of easily identifiable photographs implicate important free speech and freedom of association rights and values under the First Amendment, especially because face-identifying photographs of crowds or political protests can be captured in public without individuals' knowledge or online and through public and semi-public social media sites.

Law enforcement has already used face recognition technology at political protests. Marketing materials from the social media monitoring company Geofeedia bragged that, during the protests surrounding death of Freddie Gray, the Baltimore Police Department ran social media photos against a facial recognition database to identify protesters and arrest them.[62]

Government surveillance such as this has a very real chilling effect on Americans' willingness to engage in public debate and to associate with others whose values, religion, or political views may be considered different from their own. For example, researchers have long studied the "spiral of silence"— the significant chilling effect on an individual's willingness to publicly disclose political views when they believe their views differ from the majority.[63] Last year, research on Facebook users documented the silencing effect of participants' dissenting opinions in the wake of widespread knowledge of government surveillance—participants were far less likely to express negative views of government surveillance on Facebook when they perceived those views were outside the norm.[64]

In 2013, a large study of Muslims in New York and New Jersey found a significant

---

[61] *See* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 Minn. L. Rev. 2, 407, 415 (Dec. 2012).

[62] *Baltimore County Police Department and Geofeedia Partner to Protect the Public During Freddie Gray Riots*, *available at* https://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf.

[63] *See, e.g.*, Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, Journalism & Mass Comm. Quarterly 2016, Vol. 93(2) 296–311, *available at* http://journals.sagepub.com/doi/pdf/10.1177/1077699016630255.

[64] *See* Karen Turner, "Mass Surveillance Silences Minority Opinions, According to Study," Wash. Post (March 28, 2016) https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/mass-surveillance-silences-minority-opinions-according-to-study/?utm_term=.6d51b07dbb33.

chilling effect on First-Amendment protected activities due to police surveillance in Muslim communities.[65] Specifically, people were less inclined to attend mosques they thought were under government surveillance or to engage in religious practices in public or even to dress or grow their hair in ways that might subject them to surveillance based on their religion. People were also less likely to engage with others in their community they didn't know for fear that person would either be a government informant or a radical. Parents discouraged their children from participating in Muslim social, religious, or political movements. Business owners took conscious steps to mute political discussion by turning off Al-Jazeera in their stores. And activists self-censored their comments on Facebook.[66]

These examples show the very real risks to First Amendment protected speech and activities from excessive government surveillance—especially when that speech represents the minority viewpoint. While we don't yet appear to be at point where face recognition is being used broadly to monitor the public, we are at a stage where the government is building out the databases to make that monitoring possible. It is important to place meaningful checks on government use of face recognition now before we reach a point of no return.

D. NGI Disproportionately Impacts People of Color

The false-positive risks discussed above could also disproportionately impact African Americans and other people of color.[67] Research—including research jointly conducted by one of FBI's senior photographic technologists—found that face recognition misidentified African Americans and ethnic minorities, young people, and women at higher rates than whites, older people, and men, respectively.[68] Due to years of well-

---

[65] Diala Shamas & Nermeen Arastu, *Mapping Muslims: NYPD Spying and its Impact on American Muslims* (March 11, 2013) http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

[66] *Id.*

[67] Nellie Bowles, *'I think my blackness is interfering': does facial recognition show racial bias?*, The Guardian (April 8, 2016) *available at* https://www.theguardian.com/technology/2016/apr/08/facial-recognition-technology-racial-bias-police.

[68] *See* B. F. Klare, M. J. Burge, J. C. Klontz, R. W. Vorder Bruegge and A. K. Jain, "Face Recognition Performance: Role of Demographic Information," in,*IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1789-1801 (Dec. 2012) http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6327355&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Ficp.jsp%3Farnumber%3D6327355. *See also* Clare Garvie & Jonathan Frankle, "Facial-Recognition Software Might Have a Racial Bias Problem," *The Atlantic* (Apr. 7, 2016)

documented racially-biased police practices, all criminal databases—including mugshot databases—include a disproportionate number of African Americans, Latinos, and immigrants.[69] These two facts mean people of color will likely shoulder exponentially more of the burden of NGI's inaccuracies than whites.

False positives can alter the traditional presumption of innocence in criminal cases by placing more of a burden on suspects and defendants to show they are *not* who the system identifies them to be. This is true even if a face recognition system such as NGI offers several results for a search instead of one, because each of the people identified could be brought in for questioning, even if there is nothing else linking them to the crime. Former German Federal Data Protection Commissioner Peter Schaar has noted that false positives in facial recognition systems pose a large problem for democratic societies. "[I]n the event of a genuine hunt, [they] render innocent people suspects for a time, create a need for justification on their part and make further checks by the authorities unavoidable."[70]

NGI's face recognition accuracy problems will also unfairly impact African American and minority job seekers who must submit to background checks. Employers regularly rely on FBI's data when conducting background checks. If job seekers' faces are matched mistakenly to mug shots in the criminal database, they could be denied employment through no fault of their own. And even if job seekers are properly matched to a criminal mug shot, minority job seekers will be disproportionately impacted due to the notorious unreliability of FBI records as a whole. At least 50 percent of FBI's arrest records fail to include information on the final disposition of the case—whether a person was convicted, acquitted, or if charges against them were dropped.[71] Because at least 30 percent of

---

http://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/.

[69] *See* NAACP, Criminal Justice Fact Sheet (2009) *available at* https://donate.naacp.org/pages/criminal-justice-fact-sheet.

[70] Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, 37, N.Y.U. (April 2009) http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf.

[71] *See* Madeline Neighly & Maurice Emsellem, *WANTED: Accurate FBI Background Checks for Employment*, National Employment Law Project (July 2013) *available at* http://www.nelp.org/content/uploads/2015/03/Report-Wanted-Accurate-FBI-Background-Checks-Employment.pdf. *See also* Ellen Nakashima, "FBI Wants to Exempt Its Huge Fingerprint and Photo Database from Privacy Protections," *Washington Post* (June 30, 2016) https://www.washingtonpost.com/world/national-security/fbi-wants-to-exempt-its-huge-fingerprint-and-photo-database-from-privacy-protections/2016/05/31/6c1cda04-244b-11e6-8690-f14ca9de2972_story.html (noting

people arrested are never charged with or convicted of any crime, this means a high percentage of the FBI's records incorrectly indicate a link to crime. If these arrest records are not updated with final disposition information, hundreds of thousands of Americans searching for jobs could be prejudiced and lose work. And due to disproportionately high arrest rates, this uniquely impacts people of color.

E. FBI Has Failed to Ensure Face Recognition Data are Protected from Internal and External Security Breaches

The many recent security breaches, email hacks, and reports of falsified data—including biometric data—show that the government must have extremely rigorous security measures and audit systems in place to protect against data loss. Just this past year, news media were consumed with stories of hacks into email and government systems, including into United States political organizations and online voter registration databases in Illinois and Arizona.[72] In 2015, hackers were able to steal sensitive data stored in Office of Personnel Management databases on more than 25 million people.[73] These data included biometric information as well as addresses, health and financial history, travel data, and data on people's friends and neighbors. It has been described as the largest cyberattack into United States government systems, and even FBI Director James Comey called the breach "a very big deal."[74] More than anything, though, these breaches exposed the vulnerabilities in government systems to the public—vulnerabilities that the United States government appears to have known for almost two decades might exist.[75]

---

that, according to FBI, "43 percent of all federal arrests and 52 percent of all state arrests — or 51 percent of all arrests in NGI — lack final dispositions").

[72] *See, e.g.,* Tracy Connor, et al., *U.S. Publicly Blames Russian Government for Hacking*, NBC News (Oct. 7, 2016) http://www.nbcnews.com/news/us-news/u-s-publicly-blames-russian-government-hacking-n662066.

[73] Julie Hirschfeld Davis, "Hacking of Government Computers Exposed 21.5 Million People," *N.Y. Times* (July 9, 2015) http://www.nytimes.com/2015/07/10/ us/office-of-personnel-management-hackers-got-data-of-millions.html. *See also, e.g.,* David Stout and Tom Zeller Jr., "Vast Data Cache About Veterans Is Stolen," *N.Y. Times* (May 23, 2006), https://www.nytimes.com/2006/05/23/washington/23identity.html; *see also* European Parliament News, *MEPs question Commission over problems with biometric passports* (Apr. 19, 2012) (noting that "In France 500,000 to 1 million of the 6.5 million biometric passports in circulation are estimated to be false, having been obtained on the basis of fraudulent documents.") http://www.europarl.europa.eu/news/en/headlines/content/20120413STO42897/html/MEPs-question-Commission-over-problems-with-biometric-passports.

[74] *Id.*

[75] *Id.*

Vulnerabilities exist from insider threats as well. Past examples of improper and unlawful police use of driver and vehicle data suggest face recognition data will also be misused. For example, in 1998, a Washington, D.C., police officer "pleaded guilty to extortion after looking up the license plates of vehicles near a gay bar and blackmailing the vehicle owners."[76] In 2008, the Virginia State Police used automated license plate readers to scan the plates of all vehicles entering facilities for Palin and Obama rallies.[77] In 2010, Immigration and Customs Enforcement enlisted local police officers to use license plate readers to gather information about gun-show customers.[78] Four Utah police officers were disciplined for misusing a confidential database.[79] Between 2014 and 2015, Florida's Department of Highway Safety and Motor Vehicles reported about 400 cases of improper use of its Driver and Vehicle Information Database.[80] And a 2011 state audit of law enforcement access to driver information in Minnesota revealed "half of all law-enforcement personnel in Minnesota had misused driving records."[81]

Officers may also access data to provide information to others unaffiliated with the police. For example, in 2014, two New York police officers were indicted after they were reportedly paid to tap into a confidential law enforcement database to obtain personal information about potential witnesses.[82] A Phoenix, Arizona officer "gave a woman involved in a drug and gun-trafficking investigation details about stolen cars in exchange

---

[76] Julia Angwin & Jennifer Valentino-DeVries, *New Tracking Frontier: Your License Plates*, Wall St. J. (Sept. 29, 2012), http://online.wsj.com/news/articles/SB10000872396390443995604578004723603576 29.

[77] Letter from First Sergeant Bobbie D. Morris to First Sergeant Alvin D. Blankenship on Division Seven Heat Operations (Mar. 18, 2009), *available at* http://www.thenewspaper.com/rlc/docs/2013/va-alpr.pdf.

[78] Devlin Barrett, *Gun-Show Customers' License Plates Come under Scrutiny*, Wall St. J. (Oct. 2, 2016), http://www.wsj.com/articles/gun-show-customers-license-plates-come-under-scrutiny-1475451302.

[79] Sadie Gurman & Eric Tucker, *Across U.S., Police Officers Abuse Confidential Databases*, Salt Lake Tribune (Sept. 28, 2016) http://www.sltrib.com/home/4407962-155/ap-across-us-police-officers-abuse.

[80] *Id.*

[81] Chris Francescani, *License to Spy,* Medium (Dec. 1, 2014), https://medium.com/backchannel/the-drive-to-spy-80c4f85b4335.

[82] Benjamin Weiser, *2 Former New York Police Officers Misused Database, U.S. Says,* N.Y. Times (Oct. 22, 2014), http://www.nytimes.com/2014/10/23/nyregion/us-accuses-2-former-police-officers-of-abusing-a-confidential-database.html?

for arranging sexual encounters for him."[83] And police have provided license plate data to reporters.[84]

Many of the recorded examples of database misuse involve male officers targeting women. For example, in Florida, an officer breached the driver and vehicle database to "look up a local bank teller he was reportedly flirting with."[85] More than 100 other Florida officers accessed driver and vehicle information for a female Florida state trooper after she pulled over a Miami police officer for speeding.[86] In Ohio, officers looked through the database to find information on an ex-mayor's wife, along with council people and spouses. [87] In Illinois, a police sergeant suspected of murdering two ex-wives used police databases to check up on one of his wives before she disappeared.[88]

It is unclear whether federal agencies have done much in the years before and after the OPM hack to improve the security of their systems. In 2007, the GAO specifically criticized FBI for its poor security practices. GAO found, "[c]ertain information security controls over the critical internal network reviewed were ineffective in protecting the confidentiality, integrity, and availability of information and information resources."[89]

---

[83] Gurman & Tucker, *Across U.S., Police Officers Abuse Confidential Databases.*

[84] Dave Maass, *Mystery Show Debunks License Plate Privacy "Myth,"* EFF (June 15, 2015), https://www.eff.org/deeplinks/2015/06/mystery-show-podcast-debunks-license-plate-privacy-myth.

[85] Amy Pavuk, *Law-Enforcer Misuse of Driver Database Soars*, Orlando Sentinel (Jan. 22, 2013) http://articles.orlandosentinel.com/2013-01-22/news/os-law-enforcement-access-databases-20130119_1_law-enforcement-officers-law-enforcers-misuse; *see also* Kim Zetter, *Cops Trolled Driver's License Database for Pic of Hot Colleague*, WIRED (Feb 23, 2012), https://www.wired.com/2012/02/cop-database-abuse/.

[86] Dave Elias, *Deputy Fired for Misusing Driver's License Database*, NBC2 (April 24, 2014) http://www.nbc-2.com/story/25334275/deputy-fired-for-improperly-accessing-info-about-governor-nbc2-anchors-others

[87] Eric Lyttle, *Fairfield County Grand Jury Indicts Two over Misuse of Database for Police*, Columbus Dispatch (April 24, 2015), http://www.dispatch.com/content/stories/local/2015/04/23/sugar-grove-police-indicted.html.

[88] Brad Flora, *What Do the Cops Have on Me?*, Slate (Dec 4, 2007), http://www.slate.com/articles/news_and_politics/explainer/2007/12/what_do_the_cops_have_on_me.html.

[89] Government Accountability Office, Information Security: FBI Needs to Address Weaknesses in Critical Network, GAO-07-368 (April 2007) http://www.gao.gov/new.items/d07368.pdf.

Given this and the fact that FBI intends to retain personal data in NGI for the length of a person's life plus seven years,[90] FBI must do more to explain why it needs to collect so much sensitive biometric and biographic data, why it needs to maintain it for so long, and how it will safeguard the data from the data breaches we know will occur in the future.

VI. Despite the Serious Issues Outlined Above, FBI has Proposed Exempting Face Recognition Data from Key Provisions of the Privacy Act

FBI proposes to exempt much of the NGI database from three key provisions of the Privacy Act: (1) the right to access records maintained on oneself; (2) the right to ensure that those records are maintained accurately and to be able to correct inaccuracies; and (3) the right to know with whom one's data are being shared.

FBI recognizes, as it must, that the Privacy Act not only requires it to maintain accurate records but also to ensure that the information it disseminates to other federal and non-federal agencies is "accurate, complete, timely and relevant."[91] FBI states that it takes this obligation seriously.[92] Nevertheless, FBI recognizes both that a significant percentage of its data is already inaccurate or out of date[93] and that face recognition is not necessarily reliable as an identification tool.[94] This means FBI has already failed to meet its legal duties under the Privacy Act.

FBI's proposed exemptions seek to prevent Americans from ever knowing exactly what data the Bureau maintains on them and shares with other agencies. And, by seeking to remove any judicial remedy, the exemptions attempt to prevent Americans from ensuring that the data the Bureau maintains is "accurate, complete, timely and relevant."

This has real-world consequences. For example, a few years ago, due to notoriously inaccurate and out-of-date immigration and arrest records,[95] approximately 3,600 United

---

[90] *See* Proposed FBI NGI SORN, "RETENTION AND DISPOSAL."

[91] 2015 FBI Interstate Photo System PIA.

[92] FBI & DOJ, Notice of Proposed Rulemaking, 81 Fed. Reg. 27288 (May 5, 2016).

[93] *See* Ellen Nakashima, "FBI Wants to Exempt Its Huge Fingerprint and Photo Database from Privacy Protections," *Washington Post* (June 30, 2016).

[94] 2015 FBI Interstate Photo System PIA.

[95] *See generally* Joan Friedland, National Immigration Law Center, *INS Data: The Track Record*, *available at* www.nilc.org/document.html?id=233 (citing multiple Government Accountability Office and Inspector General reports on inaccuracies in immigration records). These problems persist. *See generally, e.g,* U.S. Government Accountability Office (GAO), *Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain*, GAO-11-146 (Jan. 18, 2011), *available at*

States citizens were caught up in the "Secure Communities" program—a program that resulted in detention and deportation for thousands of people.[96] FBI's proposed exemptions would take away the ability for citizens in cases such as these to learn whether the inaccurate records leading to their detention came from the Bureau. The proposed exemptions also seek to remove those citizens' rights to force FBI to correct and update its records.

Given the vast scope of data included in NGI, the impact that inaccuracies in that data would have on Americans' lives, and the possibility FBI and other agencies may use this data—in violation of the Privacy Act—to monitor First Amendment protected activities, FBI should not be allowed to exempt NGI from the Privacy Act.

VII. Proposals for Change

The over-collection of face recognition data has become a real concern, but there are still opportunities—both technological and legal—for change.

Given the current uncertainty of Fourth Amendment jurisprudence in the context of face recognition and the fact that the technology is undergoing "dramatic technological change,"[97] legislative action could be a good solution to curb the over-collection and over-use of face recognition data in society, both now and in the future. If so, the federal government's response to two seminal wiretapping cases in the late 60s could be used as a model.[98] In the wake of *Katz v. United States*[99] and *New York v. Berger*,[100] the federal

---

http://www.gao.gov/products/GAO-11-146 (noting errors in USCIS's e-Verify system and difficulties in correcting those errors).

[96] *See, e.g.*, Aarti Kohli, et al. *Secure Communities by the Numbers: An Analysis of Demographics and Due Process*, at p.4, Chief Justice Earl Warren Institute on Law and Social Policy, UC Berkeley School of Law (Oct. 2011), *available at* www.law.berkeley.edu/files/Secure_Communities_by_the_Numbers.pdf.

[97] *United States v. Jones*, 565 U.S. 400, 427 (2012) (Alito, J., concurring).

[98] In Justice Alito's concurrence in *Jones*, he specifically referenced post-*Katz* wiretap laws and called out for legislative action, noting "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative." *Id.* at 427-28, 429.

[99] 389 U.S. 347 (1967).

[100] 388 U.S. 41 (1967). *Berger* was unique in that it struck down a state wiretapping law as facially unconstitutional. In striking down the law, the Court laid out specific principles that would make a future wiretapping statute constitutional under the Fourth Amendment.

government enacted the Wiretap Act,[101] which lays out specific rules that govern federal wiretapping, including the evidence necessary to obtain a wiretap order, limits on a wiretap's duration, reporting requirements, a notice provision, and also a suppression remedy that anticipates wiretaps may sometimes be conducted unlawfully.[102] Since then, law enforcement's ability to wiretap a suspect's phone or electronic device has been governed primarily by statute rather than Constitutional case law.

Congress could also look to the Video Privacy Protection Act (VPPA),[103] enacted in 1988, which prohibits the "wrongful disclosure of video tape rental or sale records" or "similar audio-visual materials," requires a warrant before a video service provider may disclose personally identifiable information to law enforcement, and includes a civil remedies enforcement provision.

If legislation or regulations are proposed in the face recognition context, the following principles should be considered to protect privacy and security. These principles are based in part on key provisions of the Wiretap Act and VPPA and in part on the Fair Information Practice Principles (FIPPs), an internationally recognized set of privacy protecting standards.[104]

Limit the Collection of Data—The collection of face recognition data should be limited to the minimum necessary to achieve the government's stated purpose. For example, the government's acquisition of face recognition from sources other than directly from the individual to populate a database should be limited. The government should not obtain face recognition data en masse to populate its criminal databases from sources such as state DMV records, where the biometric was originally acquired for a non-criminal purpose, or from crowd photos or data collected by the private sector. Techniques should

---

[101] 18 U. S. C. §§2510–2522.

[102] *See, e.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 851-52 (2004); 18 U.S.C. § 2515.

[103] 18 U.S.C. § 2710.

[104] *See* Privacy Act of 1974, 5 U.S.C. § 552a (2010). *See also* Organization for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) available at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html. The full version of the FIPPs as used by DHS includes eight principles: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. *See* Hugo Teufel III, Chief Privacy Officer, DHS, Mem. No. 2008-01, Privacy Policy Guidance Memorandum (Dec. 29, 2008), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

also be employed to avoid over-collection of face prints (such as from security cameras or crowd photos) by, for example, scrubbing the images of faces that are not central to an investigation.

Define Clear Rules on the Legal Process Required for Collection—Face recogntion should be subject to clear rules on when it may be collected and which specific legal processes—such as a warrant based on probable cause—are required prior to collection. Collection and retention should be specifically disallowed without legal process unless the collection falls under a few very limited and defined exceptions. For example, clear rules should be defined to govern when law enforcement or similar agencies may collect face recognition images from the general public without their knowledge.

Limit the Amount and Type of Data Stored and Retained—A face print can reveal much more information about a person than his or her identity, so rules should be set to limit the amount of data stored. Retention periods should be defined by statute and should be limited to no longer than necessary to achieve the goals of the program, with a high priority placed on deleting data. Data that is deemed to be "safe" from a privacy perspective today could become highly identifying tomorrow. For example, a data set that includes crowd images could become much more identifying as technology improves. Similarly, data that was separate and siloed or unjoinable today might be easily joinable tomorrow. For this reason retention should be limited, and there should be clear and simple methods for a person to request removal of his or her biometric from the system if, for example, the person has been acquitted or is no longer under investigation.[105]

Limit the Combination of More than One Biometric in a Single Database—Different biometric data sources should be stored in separate databases. If face recognition needs to be combined with other biometrics, that should happen on an ephemeral basis for a particular investigation. Similarly, biometric data should not be stored together with non-biometric contextual data that would increase the scope of a privacy invasion or the harm that would result if a data breach occurred. For example, combining facial recognition technology from public cameras with license plate information increases the potential for tracking and surveillance. This should be avoided or limited to specific individual investigations.

Define Clear Rules for Use and Sharing—Biometrics collected for one purpose should not be used for another purpose. For example, photos taken in a non-criminal context, such as for a drivers license, should not be shared with law enforcement without proper

---

[105] For example, in *S. and Marper v. United Kingdom*, the European Court of Human Rights held that retaining cellular samples and DNA and fingerprint profiles of people acquitted or people who have had their charges dropped violated Article 8 of the European Convention on Human Rights. *S. and Marper. v. United Kingdom*, App. Nos. 30562/04 and 30566/04, 48 Eur. H.R. Rep. 50, 77, 86 (2009).

legal process. Similarly, face prints collected for use in a criminal context should not automatically be used or shared with an agency to identify a person in an immigration context. Face recognition should not be used to identify and track people in real time without a warrant. And private sector databases should be required to obtain user consent before enrolling people into any face recognition system.

Enact Robust Security Procedures to Avoid Data Compromise—Because biometrics cannot be changed, data compromise is especially problematic. Using traditional security procedures, such as basic access controls that require strong passwords and exclude unauthorized users, as well as encrypting data transmitted throughout the system, is paramount. However security procedures specific to biometrics should also be enacted to protect the data. For example, data should be anonymized or stored separate from personal biographical information. Strategies should also be employed at the outset to counter data compromise after the fact and to prevent digital copies of biometrics. Biometric encryption[106] or "hashing" protocols that introduce controllable distortions into the biometric before matching can reduce the risk of problems later. The distortion parameters can easily be changed to make it technically difficult to recover the original privacy-sensitive data from the distorted data, should the data ever be breached or compromised.[107]

Mandate Notice Procedures—Because of the real risk that face prints will be collected without a person's knowledge, rules should define clear notice requirements to alert people to the fact that a face print has been collected. The notice provision should also make clear how long the data will be stored and how to request its removal from the database.

Define and Standardize Audit Trails and Accountability Throughout the System—All database transactions, including face recognition input, access to and searches of the system, data transmission, etc. should be logged and recorded in a way that assures accountability. Privacy and security impact assessments, including independent certification of device design and accuracy, should be conducted regularly.

Ensure Independent Oversight—Government entities that collect or use face recognition must be subject to meaningful oversight from an independent entity. Individuals whose data are compromised, whether by the government or the private sector should have a strong and meaningful private right of action.

---

[106] *See, e.g.,* Information and Privacy Commissioner, Ontario, Canada, *Privacy-Protective Facial Recognition: Biometric Encryption—Proof of Concept* (Nov. 2010), available at www.ipc.on.ca/images/Resources/pbd-olg-facial-recog.pdf.

[107] *See, e.g.,* Center for Unified Biometrics and Sensors, "Cancellable Biometrics," SUNY Buffalo, http://www.cubs.buffalo.edu/cancellable.shtml (last visited Mar. 15, 2012).

VIII. Conclusion

Face recognition and its accompanying privacy and civil liberties concerns are not going away. Given this, it is imperative that government act now to limit unnecessary data collection; instill proper protections on data collection, transfer, and search; ensure accountability; mandate independent oversight; require appropriate legal process before collection and use; and define clear rules for data sharing at all levels. This is important to preserve the democratic and constitutional values that are bedrock to American society.

Thank you once again for the invitation to testify. I am happy to respond to questions.

Respectfully submitted,

Jennifer Lynch
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
jlynch@eff.org

Chairman CHAFFETZ. Thank you. I appreciate it.

We'll now recognize the ranking member, Mr. Cummings, for 5 minutes.

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

And I want to welcome our witnesses here today.

Let me start by acknowledging that facial recognition technology provides law enforcement officials with an innovative and valuable tool to identify suspects and criminals, which helps keep all of us safe. We all know that.

The FBI has told us that this technology helps them identify and apprehend criminals and bring them to justice. I strongly believe that our law enforcement authorities should have access to the most advanced crime-fighting tools available to protect our communities.

But serious questions have been raised in your testimony today already about the accuracy of facial recognition technology, its disparate impact on certain populations, and its use against law-abiding Americans.

To help our law enforcement authorities do their job as effectively as possible while at the same time protecting the rights of constituents, we need to examine these questions head on because they are very, very significant. So I am thankful that we are having this discussion today.

There are three key points that I would like to address today. The first is that whole question of accuracy. Last year, the Government Accountability Office issued its report with a very significant warning. The GAO reported that the FBI has, and I quote, "limited information on the accuracy of its face recognition technology capabilities," end of quote.

The GAO also warned that the FBI did not assess how often these searches, and I quote, "erroneously match a person to the database that falsifies the rate," end of quote. That's a big problem.

As one of the Members of Congress who live in the inner city of Baltimore, where I have seen the impact of police, certain police tactics, with regard to African-American males and having been an African-American male for 66 years on this Earth, I can tell you I have a lot of concerns about this.

GAO made a series of recommendations, including proposing that the FBI conduct more testing to, and I quote, "help ensure that the system is capable of producing sufficiently accurate search results." That seems like a reasonable request. Unfortunately, the Department of Justice disputed the need for more accuracy testing and maintains that current testing is adequate.

Second is the question of disparate treatment of some Americans. In 2012, senior technology experts with the FBI coauthored a study finding that some of the leading algorithms used in face recognition systems were 5 percent to 10 percent less accurate on African Americans as compared to Caucasians.

Similarly, on October 18, 2016, the Center on Privacy & Technology at the Georgetown University Law Center issued a report finding that, I quote, "African Americans are disproportionately likely to be subject to police face recognition," end of quote.

According to these reports, if you're Black, you're more likely to be subjected to this technology, and the technology is more likely

to be wrong. That's a hell of a combination, particularly when you're talking about subjecting somebody to the criminal justice system. We need to let this sink in.

For these reasons, the center made a very sensible recommendation, that the FBI simply test the system for racial bias. Why can't we do that? What's the problem? In response, the FBI claims there's no need to test for racial bias because the system is race-blind. I disagree. I disagree.

Walk around this country as a Black man, in this country, and this kind of—don't get me wrong. I believe strongly that police should have every tool they need to solve crime. But I'm telling you: we have seen some things in Baltimore where the African-American community is almost like a guinea pig sometimes. Say, okay, we believe all the crime is happening here, so everything goes there. And this is the neighborhood I live in, that I go home to every night. So the response is very troubling.

I'm almost finished, Mr. Chairman.

Rather than conducting testing that would show whether or not these concerns have merit, the FBI chooses to ignore growing evidence that the technology has a disproportionate impact on African Americans.

Third is the question of protecting other rights of the American people, including their privacy rights, their civil liberties, and their right to free speech. And I want to applaud the chairman for constantly raising these kinds of issues because they are very important.

I've said many times that sometimes we take for granted this democracy that we have. We take it for granted. It has been working so well that we assume we can—it will be here forever. But we have to guard it every day. And I think that, when you see things that begin to chip away at it, you have to pause and say: "Wait a minute. Hold on. Where are we going here?"

And so, according to GAO, law enforcement authorities now have the ability to search more than 400 million photos. There does not have to be a warrant. There does not even have to be probable cause. They search not only criminal mugshots but photos of law-abiding citizens that are submitted when they apply for jobs, passports, and even driver's licenses.

I doubt many Americans realize that when they go down to the DMV to get their driver's licenses, their photos could be made part of a database that can be searched by the FBI. The Center on Privacy & Technology estimates that 80 percent of photos in the FBI's network of facial recognition searches are people who have never been accused of a single crime.

Last year, the ACLU reported that the Baltimore Police Department used this technology against crowds of people who were protesting against police misconduct as a result of the death of Freddie Gray. Now, I was in the crowd. I was in the crowd, night after night, six nights in a row. So I guess they've got my photo. And they probably have a lot of other photos. There were a lot of people there in the crowd with us in Baltimore who have never been arrested, who have never committed a crime, but yet still they're subject to this.

Now, understand, I guess my concern is that if we are going to, again, use tools, it seems to me that we would do everything in our power to make sure that those tools are used in a fair way, that we are testing for accuracy, and that there's not bias against one part of our population.

And so I'm glad that we're having the hearing today. I'll have some questions later, but thank you, Mr. Chairman.

And I yield back.

Chairman CHAFFETZ. I thank the gentleman.

All right. I'll now recognize myself for 5 minutes and then members will ask questions.

Ms. Del Greco, the GAO report asserts that the FBI failed, even though it's directed by law, to put out the Privacy Impact Assessment. Why did the FBI not fulfill the law, the requirement of the law, and why did you not update the Privacy Impact Assessment? You have to put the——

Ms. DEL GRECO. Thank you. Thank you, Mr. Chairman.

I will defer to DOJ on that question.

Chairman CHAFFETZ. What do you mean "defer to DOJ"? You are DOJ. So what do you mean "defer"?

Ms. DEL GRECO. The Privacy Impact Assessment was submitted to the Department. I will defer to them for a response.

Chairman CHAFFETZ. I'm sorry. We're having a hearing to ask you the questions, and the DOJ put you up there. You seem like a very nice person, but you're supposed to be the one to answer that question. What do you mean "defer"?

Ms. DEL GRECO. As I've stated, the Privacy Impact Assessment was submitted, and they——

Chairman CHAFFETZ. Years late, right?

Director Maurer, do you want to comment on this?

Ms. MAURER. Yes, that's correct. It was submitted years after both systems were being used for real-world use.

Chairman CHAFFETZ. So here's the problem: You're required by law to put out a privacy statement, and you didn't. And now we're supposed to trust you with hundreds of millions of peoples' faces in a system that you couldn't protect, even with the 702 issue. Now, we're talking about Mr. Flynn and how he was unmasked and all that, and there can be political gyrations, but set the name aside, and Donald Trump and all that.

But even in that most stringent circumstance where they're looking at information, somebody decided to take off that veil and release that out to the public. And we're supposed to—and the Office of Personnel Management had tens of millions of Federal workers who had information where—and some of it included fingerprints and other types of things, and that was stolen and let out, and those people are having to suffer the consequences the rest of their lives. Why should we trust you?

Ms. DEL GRECO. The privacy was part of the entire process in the development phases of the Interstate Photo System.

Chairman CHAFFETZ. I know, but—okay. The point is, that the GAO has rightfully, I think, pointed out, the FBI was required by law to comply with the law—you are part of the Department of Justice—and you failed to do so. I hope you can see how this is a problem.

Ms. DEL GRECO. A Privacy Impact Assessment was initiated in 2008 on a pilot project for a proof of concept. Throughout the whole process, our privacy attorney was being advised of the changes that were being made in the development.

Chairman CHAFFETZ. Yeah, well, we don't believe you, and the second part of that is you're supposed to make that public. And the failure here is, years after it was supposed to be made public, you didn't do it. You were using it in a real-world circumstance. You were actually using it and didn't issue the statement.

Let me move on. You said a couple of times, Ms. Del Greco, in your testimony that this was a, and I quote, "an investigative lead," that everybody should relax; it's just being used for an investigative lead. Correct?

Ms. DEL GRECO. That is correct.

Chairman CHAFFETZ. So why not collect everybody's fingerprints? That would be an investigative lead, right? Wouldn't that be easier if you had everybody's fingerprints? Why not collect everybody's fingerprints?

Ms. DEL GRECO. We use fingerprint technology as a positive identification, and we still do today.

Chairman CHAFFETZ. But why not collect them all in advance? I mean, that would be easier, right? If you have a database, you collect them all in advance; then, when you go and you pull off somebody's fingerprints, you've got a database, right? Why not do that?

Ms. DEL GRECO. Fingerprints are collected with a criminal mugshot for an arrested purpose, for a law enforcement purpose.

Chairman CHAFFETZ. Yeah. But you see the difference, right, somebody is actually arrested; then they take their fingerprints. Somebody who is actually convicted, then you collect the—then you have your fingerprints. But why not get them all in advance? What if we had all 330 million Americans' fingerprints in advance? That would be easier, wouldn't it? It would be easier, right? That's a question.

Ms. DEL GRECO. We collect fingerprints with the criminal law enforcement purpose only.

Chairman CHAFFETZ. Right. Right. Why not collect everybody's DNA? How about when everybody's born in the United States, we take a little vile, a sample of blood? Why don't we do that? Then we'd have everybody's DNA. And then when there's a crime, then we could go back and say, "Oh, well, let's collect that DNA, and now we have 330 million Americans." That would be easier. Wouldn't it?

Ms. DEL GRECO. I'm not at liberty to speak about the DNA collection.

Chairman CHAFFETZ. This is different. See, this is how DNA is a valuable investigative tool. Fingerprints are a valuable investigative lead and tool. But what scares me is the FBI and the Department of Justice proactively trying to collect everybody's face, and then having a system with a network of cameras where, if you go out in public, that too can be collected and then used in the wrong hands, nefarious hands, somebody in government misusing it. It does scare me.

Are you aware of any other country that does this? Anybody on this panel. Is there any other country that's doing this?

Let me ask you one other thing, and I've gone past my time here—past my time here. Do you have plans to match this database up with anything that's posted on social media? So, in other words, if you go up on Instagram, Facebook, Snapchat, and whatever the next new technology is, are you collecting that information that is out there on social media?

Ms. DEL GRECO. No, we are not. The only information the FBI has and has collected in our database are criminal mugshot photos. We do not have any other photos in our repository.

Chairman CHAFFETZ. That's not true. You are not collecting driver's licenses?

Ms. DEL GRECO. We do not have driver's license photos in our repository at the FBI.

Chairman CHAFFETZ. Does anybody care to weigh in on this? Mr. Bedoya?

Mr. BEDOYA. Sure, Mr. Chairman. I think this is a technicality. Who owns and operates a database matters a lot less than who uses it and how it's used. The FBI has access to now 18 States' driver's license photos that either can run those searches or request them. We're talking more than a third of all Americans. So the FBI does have access to these photos. They searched them tens of thousands of times and, apparently, by GAO's testimony, never audited those searches for misuse.

Chairman CHAFFETZ. Would you disagree with that, Ms. Del Greco?

Ms. DEL GRECO. We have access to the data. We do not maintain the data in our repository. And the access we have is pursuant to the provision in the Driver's Protection Act within the State, accordance with Federal law.

Chairman CHAFFETZ. Does anybody else care to weigh in on this topic? Ms. Lynch?

Ms. LYNCH. Thank you, Mr. Chairman.

I would also add that the FBI has civil photos in its repository. So it's not just relying on driver's license databases, but it also has access to civil photos in its own NGI–IPS database. These photos may in the future come from background checks that people submit to as trying to get employment or as a licensing requirement, but the database is not limited to just mugshot photos.

Mr. CUMMINGS. Would the chairman yield?

Chairman CHAFFETZ. Sure.

Mr. CUMMINGS. Just to clear up, Ms. Del Greco, when the chairman asked you about what photos you had, you said over and over again, we have just a mugshot—what did she say?

Chairman CHAFFETZ. Just the criminal.

Mr. CUMMINGS. I just feel that you could've been a little—after we got this more clarification, seemed like you would have told us that, what they just told us. I mean, it just seems—I mean, I don't know how he feels, but if I was left with your answer and didn't have clarification, I would have assumed that that's it.

But they were able to clarify, these other two witnesses, that you have access to all kinds of photos. Hello? I just think it is a little unfair to the committee. I usually don't do this. But it just—it kind

of left me not feeling very good. And I'm sure the chairman probably felt the same way.

Chairman CHAFFETZ. So, if they are in your database or you own that database and own those photos, what other databases are you also tapping into at will?

Ms. DEL GRECO. We do not search the civil photos that are in our repository. They are not located in the Interstate Photo System. We only search the criminal mugshots that we have in our repository. We are not authorized; they are not searchable, the civil photos.

We also retain the investigative photo from the FBI agent, but those are not—the civil photos are not searchable.

Chairman CHAFFETZ. Well, I'm going to flesh this out. I'm well past my time. So we'll continue to flesh this out.

But let's go to Mr. Lynch of Massachusetts now.

Mr. LYNCH OF MASSACHUSETTS. Thank you, Mr. Chairman and Ranking Member, for your work on this.

I appreciate the presence and testimony of our witnesses.

I don't think it's a stretch to say that the majority of Americans today feel that the rapid advances in surveillance technology have far outpaced the ability of Congress to protect the basic privacy of American citizens. And apart from the willingness of people to put some of their most intimate information online, I think there's been an aggressive development of surveillance technology that we've seen come to the forefront. And when you think about how this could change who we are as a Nation, it's very, very troubling. This country was founded on protest—it really was—and is continually reshaped by protest. And it disturbs me greatly that, whether it was the death Freddie Gray and those protests or the women's protest recently that was all over the country, millions of people, it disturbs me greatly that we're out there taking in this information.

And I fully support the suggestion of Ms. Lynch—no relation—that a warrant should be required in those cases and that, if we're going to build these databases and have this ability to surveil innocent individuals, then that is really a game-changer for this country.

The background here, Ms. Del Greco, goes back to the confidential informant programs that are run by the FBI, DEA, ATF. And we have had zero cooperation from the FBI in the tens of thousands of confidential informants that you run daily in this country.

We did get a report from the Inspector General's Office that explained that the DEA, in addition to the FBI, is operating 18,000 confidential informants. They paid $237 million to confidential informants. And we can't get information on who's getting paid for what. So, in addition, I think there's probably 15,000 to 20,000 FBI informants that are out there. And we have very little accountability as to what they are doing, who they are working for, what they are being paid for, what their prior crimes were, what their extant crimes are while they are being paid as informants. So I have zero confidence in the FBI or the DOJ, to be frank with you, of keeping this in check.

Mr. Bedoya, you talked about some of the things that might be put in place—Ms. Lynch as well. I'm certainly going to join in legislation to put a warrant requirement in on this. There are some

areas, you know—I know that we had some enhanced alerts regarding threats to our transportation system. So we put in surveillance cameras at South Station, at Union Station, because we had threats in those specific areas for limited periods of time. And I don't dispute that, on occasion, with specific threats and specific information, we should use that tool.

But, Mr. Bedoya and Ms. Lynch, what else should be included in legislation that would allow us to use this tool, this technology, while balancing the preservation of individual rights and privacy for American citizens?

Mr. Bedoya, you could start.

Mr. BEDOYA. Yes, sir. There's a couple of points, and I can go through them quickly. We need to target this powerful technology to serious criminals. And so that, in the first instance, we need to do. Secondly, we need to restrict real-time face scanning to situations like you described, very specific threats, very specific occasions. We need to make sure this technology's accurate. We need to test it publicly and independently for bias. We need safeguards to prevent against misuse and abuse. So we need audits to spot if this technology is being abused. And we need reporting like you would have for—under the Wiretap Act, where if you do a wiretap, later on, you report about it: the crime, what happened with that prosecution. So, across the board, there are reforms that could be made that are modeled on existing law and also modeled on the policies of the States represented on this committee that could be best practices and commonsense rules for the road here.

Mr. LYNCH OF MASSACHUSETTS. What about an opt-out provision for any citizen who is not suspected of a crime, to have somebody, some ombudsman, go through and delete all the pictures of people who aren't under active consideration for criminal activity? I mean, I think that's something that—innocent people should not be on this database. This is really Nazi Germany here what we're talking about. They had meticulous files on individuals, most of them of Jewish faith, and that's how they tracked their people. And I see little difference in the way people are being tracked under this, you know, just getting one wide net and collecting information on all American citizens. I think it is corrosive of our very liberty. I just appreciate your testimony.

Ms. Lynch, anything to add?

Ms. LYNCH. I think the only thing I would add to Mr. Bedoya's response is that we need to have protections to prevent the use of face recognition on First Amendment-protected activities. So, as I think that you just noted, one of the risks in using face recognition would be to identify people who are engaging in political protest, which is a bedrock value in our society, to be able to engage in political protest without the fear that the government will be identifying us and targeting us for our political beliefs. So, if any legislation is introduced, I would encourage a provision in that legislation to cover First Amendment-protected activities.

Mr. LYNCH OF MASSACHUSETTS. Thank you.

I appreciate the courtesy, and I yield back the balance of my time.

Chairman CHAFFETZ. I thank the gentleman.

I now recognize the gentleman from Michigan, Mr. Mitchell.

Mr. MITCHELL. Thank you, Mr. Chairman.

Mr. Cummings, this will be the second time in a week where I'm going to climb into the boat with you, sir.

Chairman CHAFFETZ. Uh-oh, boat analogy.

Mr. MITCHELL. My boating analogy for the day.

My older son is a police officer. He is a detective in Michigan. And as I read this, I'm, frankly, appalled. I didn't—I wasn't informed that, when my driver's license was renewed, my photograph was going to be in a repository that could be searched by law enforcement across the country. As you did your MOU with the Michigan State Police, what efforts did you take to make sure, in fact, privacy requirements were maintained?

Ms. DEL GRECO. Well, first, we looked at the State law and worked with the State to ensure that there was a State law that allowed for the use of those records for law enforcement purposes.

Mr. MITCHELL. So we made sure there was a State law that said privacy didn't matter?

Ms. DEL GRECO. It was a privacy document with regard to driver's license photos in the State.

Mr. MITCHELL. So, again, if the State said it was okay that we collected them, there's—I'm not aware of anything in the State of Michigan that said they can just provide those photos to other parties for law enforcement purposes.

Ms. DEL GRECO. We work with the State's legal counsel along with our legal counsel to ensure that the appropriate laws are in place before an MOU is drafted and approved.

Mr. MITCHELL. So law enforcement all got together and said, "It's okay, and we're going to do that."

Followup question for you, I spent 35 years in private business, and we had to comply with Federal privacy laws. We were involved in student education, student aid. I was subject to criminal and civil penalties personally as the CEO of the company if, in fact, we failed to maintain compliance to privacy laws. What civil and criminal penalties have the Department of Justice been subjected to for failure to comply with the privacy requirements?

Ms. DEL GRECO. With regard to FACE Services?

Mr. MITCHELL. Well, with regard to filing the updated privacy information that the chairman referred to. You're years late.

Ms. DEL GRECO. That I am not an expert to speak on, sir.

Mr. MITCHELL. You're not aware. So we don't know whether or not—has any action been taken for failure to move forward? You said you implemented the report. Has any action been taken for the individuals that stopped the report because it was not issued?

Ms. DEL GRECO. I have no knowledge.

Mr. MITCHELL. There are days that ignorance is bliss; I appreciate that.

Question for Mr. Bedoya, if you would, sir, is there any legal standard that law enforcement must use in order to request access to the database? I see, on page 3 of the GAO report, there is—essentially—effective, the State makes a request, and then they access the database. Is there any legal standard for access there, sir?

Mr. BEDOYA. Sure, for the FBI, the FBI can open an investigation, can run a face recognition search—for example, your face in Michigan—on mere allegation or information.

Mr. MITCHELL. How about the State agency requesting the information from the FBI and/or other States? What do they have to submit?

Mr. BEDOYA. The State agency has to have a criminal justice purpose but is not required to have reasonable suspicion to search the FBI's database.

Mr. MITCHELL. So they don't have to tell the FBI why it is they are asking for access to that database, just that they need it.

Mr. BEDOYA. I am not familiar with the exact field they need to fill out, but they do not need to meet the most minimal standard, which would be reasonable suspicion.

Mr. MITCHELL. Ms. Del Greco, can you explain that?

Ms. DEL GRECO. A State law enforcement agency must have an originating agency identifier. They have to be a criminal justice agency. In fact, for FACE Services, they have to be in a law enforcement agency. So the rules are a little bit more refined.

Mr. MITCHELL. So refined I guess, but so long as you're a law enforcement agency, you can request access to the database because they say they want it?

Ms. DEL GRECO. They have to have an agency identifier in order to do so.

Mr. MITCHELL. An agency identifier is what, please?

Ms. DEL GRECO. It's an identifier that we provide to an authorized law enforcement agency that has authorized purposes to our system.

Mr. MITCHELL. So they have to have the top secret code.

Ms. DEL GRECO. We clarify and verify that that agency is authorized to have access to our system.

Mr. MITCHELL. But, again, they haven't had to provide any indication of investigation or, as has been noted by my colleagues, a search warrant or what the investigation; it's just that they want access for some—correct?

Ms. DEL GRECO. It has to be for law enforcement purposes.

Mr. MITCHELL. Based on someone saying it is, without any documentation?

Ms. DEL GRECO. Based on their rules and their authorities within their State, yes, sir.

Mr. MITCHELL. Mr. Bedoya or Ms. Lynch, any comment on that?

Mr. BEDOYA. Sir, I can quickly comment on that. The FBI leaves it entirely to the States to decide what their policies will be for when and why they search this database above the standards that Ms. Del Greco raised. And, frankly, you know, I think we need to take a step back and ask, if this technology had been in place for the Boston Tea Party or during the 1960s civil rights protest, what would have happened then? I think this is a very serious issue across the board.

Mr. MITCHELL. Well, I think the issue goes beyond the First Amendment concerns that were expressed by Ms. Lynch and is broader. I don't want to just protect someone if they are at a political protest from being identified. The reality is we should protect everybody unless there is a valid, documented criminal justice action. Why should my photo—God knows lately it's in every place in the world, including Facebook—be subject, because I get a driver's license, to access?

And I agree with the ranking member, the comment regarding the, "Well, we don't have access to that," is disingenuous because, frankly, the FBI has access to, whether you own the database or not, to 400 million photos of Americans solely because you say you have a criminal justice reason for them. I have to tell you—and my time is expiring; I apologize, Mr. Chairman—to me, that's appalling. And I would join in making you take actions to, in fact, limit that dramatically.

I'm sorry for going over. I appreciate the patience, and I yield back, sir.

Chairman CHAFFETZ. I thank the gentleman.

We will now recognize the ranking member, Mr. Cummings.

Mr. CUMMINGS. Mr. Bedoya, last year, the Center on Privacy & Technology released a report on police facial recognition and found that, and I quote, "There is a real risk that police face recognition will be used to stifle free speech." Is that right?

Mr. BEDOYA. Certainly, I believe so. And we have a couple of instances where this has happened. You mentioned one, the Freddie Gray protests. In 2012, thanks to Freedom of Information Act requests filed by the Electronic Frontier Foundation, we saw that, in fact, FBI presentations showed how this technology could be used on Presidential campaign rallies in 2008. And so I think there's a real risk that law-abiding Americans are going to be too scared to protest because they are afraid the government is going to secretly scan and identify and track their faces.

Mr. CUMMINGS. So what steps should be taken to ensure that the technology is not used to stifle protests?

Mr. BEDOYA. I think you could have a belt-and-suspenders method, sir. The first is you need to have reasonable suspicious that someone is engaged in a crime if you are actually encountering them. So they can see you. But if you are doing this outside of the public eye against mugshots, we think that should be restricted to felonies. And if you are doing it with driver's licenses, we think that the public of the State should actually vote to approve that; otherwise, it should not be allowed. And even then, we think there should be a warrant to access that information based on probable cause. And, separately, you need to have a policy like Ohio's or like the one proposed by DHS and FBI, actually——

Mr. CUMMINGS. And I realize that Ohio is the only one that prohibits the use of facial recognition. Is that right?

Mr. BEDOYA. I wouldn't say "prohibits," sir. I would say actively discourages it, and that is a standard also proposed by DHS and FBI in a working group in——

Mr. CUMMINGS. So you would support that?

Mr. BEDOYA. Certainly, sir.

Mr. CUMMINGS. Ms. Del Greco, despite the findings and recommendations, the FBI refuses to conduct any test to determine whether the system has racially disparate error rates. If one of the FBI's own senior technology experts as well as outside groups like the center have identified evidence that these systems may be less accurate for African Americans, does that concern you?

Ms. DEL GRECO. Our requirement when we developed the Interstate Photo System did not include tone or ethnicity. It was based on the mathematical computation only.

Mr. CUMMINGS. But you didn't answer my question. I said, did that concern you?

Ms. DEL GRECO. I'm confident in the development of our use and the system that the FBI utilizes for facial recognition.

Mr. CUMMINGS. So it wouldn't bother you if a certain segment of the population was treated unfairly? I mean, you are with the FBI, right?

Ms. DEL GRECO. The responses we get back are based on the mathematical computation. And then our facial recognition examiners are highly trained then to make the final decision on whether there's a most likely candidate. It is not based on the tone or ethnicity of the candidate.

Mr. CUMMINGS. So you're still saying everything is color-blind? Ma'am?

Ms. DEL GRECO. When we get back a response from the search from a probe photo, it could be all races. It is only a mathematical computation that returns the candidate list.

Mr. CUMMINGS. Ms. Lynch, you've got to respond to that for me, please.

Ms. LYNCH. Well, I think there are a few things I'd like to respond to. I think the first is that we do have these studies that show that African Americans and young people and women are misidentified at higher rates than Whites and men and older people. And that is due to the training data that's used in face recognition systems. Most face recognition systems are developed using pretty homogeneous images of people's faces. So that means mostly Whites and men. And so the system learns from that data and doesn't learn how to identify African-American faces as well as White faces.

Mr. CUMMINGS. Can we stick a pin in that?

Ms. LYNCH. Yes——

Mr. CUMMINGS. Whoa, whoa, whoa. If we're in denial that something is—that there's a problem, going back to—I'm not saying you're denying it, but you're close—and it seems as if, with all of our expertise, with all of our great minds, we would say, "Okay, well, maybe we can improve on this." You just said that maybe there are not enough samples or whatever. My point is, is that, if we don't recognize that there is a problem, we'll never improve on it.

And I mean, I think everybody wants to make sure we're safe. We want to make sure that law enforcement has the tools they need. But at the same time, if I turn a blind eye and say, "This is color-blind," I'll never improve the system. But go ahead.

Ms. LYNCH. Well, I think that we have to look a little bit broader. We have to look, not just at the system, but also, who is doing the backup identification? So the FBI produces a ranked candidate list in response to most of the face recognition searches that are done by the States or the local agencies. Now these are automated searches. So the FBI isn't looking through those candidates and saying, "This is the most likely match." It is just the system that is looking through those candidates and saying, "This is the most likely match." And then a human has to look through those and say, "This is the person who is in the grainy surveillance camera photo that I'm trying to identify."

But the problem is not just that the system misidentifies African Americans at a higher rate but also that human ID backup fails as well. So, if a person is not properly trained in how to do the backup identification, then they may misidentify the person as well. And we know that this is even more true if the person who is doing the identification is of a different race or ethnicity than the candidate.

Mr. CUMMINGS. I think my time is up.

Thank you, Mr. Chairman.

Chairman CHAFFETZ. Thank you.

We'll now recognize Mr. Ross of Florida for 5 minutes.

Mr. ROSS. Thank you, Mr. Chairman.

I want to preface my remarks by saying that, 35 years ago, I was in the computer industry in both selling and installing computer systems. And I set that by way of example because of my friend, Mr. Lynch, has set the proposition that technology has advanced so exponentially that it has outpaced Congress' ability to, I think, really provide the protections necessary.

And this really intrigues me, this particular topic, because, Mr. Bedoya, as you talk about some of the legal protections, one thing I haven't heard is the protections granted by the Fourth Amendment to unlawful search and seizure. And I would like to bifurcate this in two ways: one, in the collection of data or the collection of facial recognition; and, two, in the application of it. And is there not an expectation of privacy? And is there an expectation of privacy that would protect the collection of any facial recognition data, given the advancements in technology and the high resolution of this equipment, that really there is no protection?

Mr. BEDOYA. So, yes, sir, I do think there is. No court has ever looked at this, which is part of the problem.

Mr. ROSS. Well, I don't think we are at that point yet. Because I can see the collection of data saying, "Okay, that"—who allowed you to collect my facial recognition? Well, you're in public.

Mr. BEDOYA. I don't think that people reasonably expect that, when they stand for a driver's license photo, that it will be searched like a criminal's fingerprint, thousands of times a month, without warrants, without oversight, without even reasonable suspicion. So I do think there is a reasonable expectation of privacy. And while the court hasn't decided it, I think in the Jones case, the Knotts case, the court has signaled that certain kinds of dragnet tracking and certain kinds of public activity and things you volunteer to other people do deserve protection.

So I do think there is a Fourth Amendment interest here and quite a strong one.

Mr. ROSS. And, Ms. Lynch, when you talked about legal protections, is it sufficient enough that I state a disclaimer that "collection of your facial recognition data may be ongoing through the surveillance cameras"? Is that what we're talking about in terms of legal protections, or is that just one level of legal protection that we are looking at?

Ms. LYNCH. I think that's just one level. And I actually don't think that that's sufficient because I think it gets back to Mr. Bedoya's point that we don't reasonably expect our image to be captured when we're walking around in public.

Mr. ROSS. But it's being done anyway, and it has been done in surveillance. I mean, cameras and you see, of course, notices that say "surveillance cameras in use on this property" or whatever. So——

Ms. LYNCH. True. There are surveillance cameras in many cities, both private and public surveillance cameras.

But I think what's different is face recognition allows people to search through those images very, very quickly. So——

Mr. ROSS. And that's the application of it, and my question is more to the collection of it. I mean, I agree there is an expectation of privacy to a degree, but if you put up a disclaimer that you're under surveillance or that surveillance is being used, does that not give the protection necessary into the collection of the data? I'm not talking about the application in the database in the search of it, but——

Ms. LYNCH. No, I don't think that gives the protection that we're looking for. And I think an example could be law enforcement says, "We are going to now search all of your email, or we are going to"——

Mr. ROSS. Right.

Ms. LYNCH. —"come into every single house, and we're just putting you on notice of that fact." That doesn't destroy a First Amendment protected interest against unlawful searches and seizures. And I think a notice on a surveillance camera also would not destroy that protection.

Mr. ROSS. Okay.

Ms. Del Greco, how secure is the database? I mean, have you had incidents of hacking or access, unauthorized access?

Ms. DEL GRECO. The Next Generation Identification System is a secure, unclassified system. It's fully accredited. It's met the Federal Information Security Management Act at the highest level.

Mr. ROSS. But no—there hasn't been any unauthorized access?

Ms. DEL GRECO. There has not.

Mr. ROSS. Okay.

Now, Mr. Romine and Mr. Hutchinson, for your input here, as I've watched technology advance and I've also—obviously, the government doesn't maintain a monopoly on technology. And, in fact, probably they are at the low end of the availability of technology. The commercial availability of facial recognition technology, is that out there?

Mr. ROMINE. It is, sir.

Mr. ROSS. And it is being utilized in the private sector, correct?

Mr. ROMINE. That's correct.

Mr. ROSS. And are we not seeing some of these same issues as to an invasion of privacy as a result of a business or some private concern utilizing it, even for marketing purposes? I can do a market analysis by facial recognition as to how many times this particular person comes into my store or comes onto my property. Realistically, you could use it for that, correct?

Mr. ROMINE. It certainly could be used for that. NIST's role is really just an independent and unbiased arbiter of the——

Mr. ROSS. But the availability exists in a commercial setting.

Mr. Hutchinson.

Mr. HUTCHINSON. Yes, sir. The availability does exist. And it is subject to consent, in most cases, because these retail outlets, these private sector customers that may use this technology, they see the sensitivity of making sure their customers are comfortable, and they certainly don't want to alienate them. But absolutely it's out there.

Mr. ROSS. Thank you. I appreciate that.

I yield back.

Chairman CHAFFETZ. The gentleman yields back.

We'll now recognize the gentleman from Virginia, Mr. Connolly, for 5 minutes.

Mr. CONNOLLY. Thank you, Mr. Chairman.

And welcome to the panel.

Mr. Bedoya, I was struck by your comments on driver's licenses. When I get my driver's license renewed and I have my picture taken, I don't do it with the presumption that that's now public property. Is that not correct?

Mr. BEDOYA. I certainly don't also.

Mr. CONNOLLY. And, therefore, it's not okay for the FBI or, for that matter—I don't know—you know, Target to purchase my picture without my consent.

Mr. BEDOYA. Or have access to it.

Mr. CONNOLLY. Or have access to it. That is your position.

Mr. BEDOYA. That is my position, yes, sir.

Mr. CONNOLLY. And presumably that would be the position of most citizens, absent an active decision that "yes, you can have it," you can't have it. Otherwise, I might have reexamined getting that driver's license.

Mr. BEDOYA. I would agree with that. I think that the citizens of the State not only should be notified and have to volunteer, but the citizens of the State should vote if they want to allow this highly invasive scanning of their faces.

Mr. CONNOLLY. Has this concept ever been challenged in a court of law?

Mr. BEDOYA. We've carefully reviewed Federal and State law specifically for face recognition cases and found none. Sometimes it's discussed tangentially or very briefly, but nothing square on, sir.

Mr. CONNOLLY. Ms. Del Greco, does the FBI have a different interpretation of the presumption of privacy with respect to the picture on a driver's license?

Ms. DEL GRECO. We utilize the Driver's Privacy Protection Act. And that is allowed through Federal law. The FBI that utilizes the driver's license photos do so with an open, active FBI investigation and is verified by the employees when they receive the photo from the FBI agent.

Mr. CONNOLLY. But you are citing an act of law. Does that act of law explicitly grant the FBI or any other Federal agency the right to the presumption of access, unlimited access apparently, to the picture on the driver's license, which is issued, I might add, by a State?

Ms. DEL GRECO. It is utilized for law enforcement purposes.

Mr. CONNOLLY. Mr. Bedoya.

Mr. BEDOYA. The Driver's Privacy Protection Act was passed in 1994. The first law enforcement face recognition system in the

country began operating 2001. The DPPA clearly contemplates sharing of individual photos with law enforcement circumstances.

Mr. CONNOLLY. Right.

Mr. BEDOYA. I don't believe it would allow what you're describing, nor has it been tested.

Mr. CONNOLLY. I agree.

Ms. Del Greco, I would suggest to you: We're not the Judiciary Committee, but I think you're on very shaky legal grounds in making the assertion you just made, that that provides you with the broad authority to have ubiquitous access to across 50 States with respect to the picture on a driver's license. I don't think it was ever contemplated, and I think Mr. Bedoya makes an awfully good point: the law was, in fact, written before this technology existed.

Who advised you to interpret the law that way, your general counsel? "You" meaning the FBI, not you personally.

Ms. DEL GRECO. Thank you. We have a team of council members that advise us. We have privacy attorneys that have been involved in every facet of the development and implementation of the Interstate Photo System and the FACE Services Unit. We also work with the attorneys within each of the States that a memorandum is developed.

Mr. CONNOLLY. Well, I just—I'm not a lawyer. This isn't the Judiciary Committee. But I know how to read a law. I know how to write laws. I do it for a living. I think it's a great stretch to take a law that preceded the technology and apply it in as sweeping a way as you do. And I just think you're going to have to get, frankly, either tested in court or you're going to have to get additional statutory authority to proceed down the road you're proceeding.

Ms. Maurer, you found that—let me see, we haven't tested the technology since 2011 prior to its deployment by the FBI. Is that correct?

Ms. MAURER. Yeah. We found that the FBI needed to do more on ensuring that it is actually making a difference in meeting its operational and mission needs. In fact, the FBI has its own requirements for conducting at least annual operational reviews. That's not been conducted with these systems.

Mr. CONNOLLY. Since 2011.

Ms. MAURER. I don't believe it's ever been conducted fully with FACE Services for IPS.

Mr. CONNOLLY. Right, fully.

Ms. MAURER. Fully.

Mr. CONNOLLY. Correct. I think your report says the last time the FBI tested the accuracy of facial recognition technology was 2011.

Ms. MAURER. Yes, that was before full deployment.That's correct.

Mr. CONNOLLY. So, Ms. Del Greco, why haven't there been more comprehensive tests in the last 6 years?

Ms. DEL GRECO. The FBI feels that the Interstate Photo System performs within the state of the art in the discipline for face matching today. If the NIST were to show extreme improvements in face recognition technology, the FBI clearly would plug in a new algorithm for the accuracy.

Mr. CONNOLLY. Well, let me read to you the conclusion of the GAO report. It says: Because of the lack of testing, there's limited

information on the accuracy of your face recognition technology capabilities.

Do you dispute that finding?

Ms. DEL GRECO. We feel that the technology we have today is—at the state of the art.

Mr. CONNOLLY. So you're just happy as a clam with the accuracy.

Ms. Maurer, do you care to comment?

Ms. MAURER. This was one of the areas of disagreement between GAO and the Department of Justice and FBI. We think it's very important for the FBI to continually test the accuracy of these systems because of all the privacy issues that this committee discussed all morning. There is criteria that exist within the FBI that they can use as a way to guide these operational reviews, both for the accuracy of the system and to ensure it meets law enforcement needs.

Mr. CONNOLLY. I think my time is up, Mr. Chairman.

Chairman CHAFFETZ. Would the gentleman yield to me?

Mr. CONNOLLY. Of course.

Chairman CHAFFETZ. Just I would like to ask unanimous consent to enter into the record two letters: one is June 23, 2016, entitled "The FBI's Use of Facial Recognition and Proposal to Exempt the Bureau's Next Generation Identification System from Privacy Act Obligation," as well as a letter that Mr. Cummings and I sent to the FBI on September 6, 2016.

Without objection, so ordered.

Chairman CHAFFETZ. This letter, Ms. Del Greco, while you say you comply with the various privacy laws, the FBI went to great lengths to exempt this database from the Privacy Act. I hope you can understand and respect our skepticism because the Privacy Act is in place to protect against these types of things, but the FBI went to great lengths to get itself exempted from the Privacy Act and that's a big part of the concern.

Mr. CONNOLLY. And, Mr. Chairman, just in this questioning—I'm so glad we're having this hearing. I think there are more questions raised than answers as to the statutory authority being cited and whether or not we need additional statutory authority to both encumber the FBI and to authorize it and to protect citizens. But there are also technology issues that have been raised here as to accuracy.

Chairman CHAFFETZ. Yes.

Mr. CONNOLLY. And if we're relying on this everywhere, that raises its own set of questions that I think we need to delve into. So I thank my friend and the ranking member for having this hearing. It's raised some really important questions.

Chairman CHAFFETZ. I thank the gentleman.

I now recognize the gentleman from Tennessee, Mr. Duncan, for 5 minutes.

Mr. DUNCAN. Well, thank you, Mr. Chairman.

And I'm sorry that other meetings prevented me from hearing the testimony of the witnesses because I'm very concerned about all of this, and I share the concerns that have been expressed by the members that I've heard here while I've been here.

I will tell you that, you know, all of our modern technology and the internet, it's got a lot of good, but it seems to me that it has

just about done away with privacy in this country. I'm wondering if we've reached a point—these cases seem to turn on the question of whether people have a reasonable expectation of privacy. And I wonder if we've reached a point where there's no reasonable expectation about privacy about anything. I remember a few years ago in this committee a company appeared before us that had downloaded 250,000 Federal income tax returns just to show that it could be done. They had been on one of the morning television shows, and they weren't in trouble, because they didn't use those returns in any way.

But now it seems that people can find out what prescriptions you've gotten, what grocery purchases you've made, your every detail about your homes. I mean, I just wonder if there's—I think we're reaching a very sad point, a very dangerous point, when we're doing away with a reasonable expectation of privacy about anything.

And I share the chairman and ranking member's concern. Ms. Del Greco, it says in this CNN report—the report criticizes the FBI for not giving the public adequate information about the programs and their privacy implications, as required under the 1974 Privacy Act. And it also says the systems have not been sufficiently tested for accuracy. We've heard about that here this morning. It seems to me that the FBI needs to step back and take another look at this GAO report and respond to it a little bit in a little more detailed fashion, because I think most people who have read this report and have heard some of these things that have been expressed here this morning would wonder if we're ending up in a Federal police state that's gotten totally out of control and really has far too much power.

I mean, the President, a month or so ago, people laughed when he said if you want to have—if you want to keep something private, don't put it into a computer; write it out and hand deliver it. And there were some sarcastic jokes about that. But, unfortunately, it's almost become true.

But I certainly commend you, Mr. Chairman, for holding this hearing and looking into this to the extent that you have because I think a lot of questions have been raised here today. Thank you very much.

Mr. CUMMINGS. Thank you very much.

Mr. Duncan, first of all, I want to associate myself with everything you just said. Before you got here, I mentioned that we really do have to guard our democracy. And I said that we sometimes I think take it for granted, and we have—when we see this chipping away with regard to privacy—and you having been a judge, you know what I'm talking about—you've got to guard this thing. And I think what happens is we get to a point where we, because we have gotten used to our way of life, we assume it's going to be that way forever. But I think it is important that we, both Republicans and Democrats, whenever we see that democracy being threatened, that very democracy that allows us to be who we are and the great Nation that we are, we have to call it and try to work together to try to address those issues. So when I heard your comments, I just wanted to let you know that I agree with you.

I yield back to the gentleman.

Mr. DUNCAN. [Presiding.] Well, thank you very much, and I do have interest in this because I was a criminal court judge for 7–1/5 years trying the felony criminal cases, and I had a very good relationship with law enforcement. But there have been some pretty serious matters discussed here this morning, and I think we need to try to do everything we possibly can to make sure that we don't just totally do away with people's expectation of privacy in this country. And we're getting close to that point, I think.

Mrs. MALONEY. I want to thank the ranking member and chairman for holding this important hearing and all of our panel.

I'd like very much to be associated with the statements on both the Republican and Democratic side. This is an issue where both are expressing a lot of concern. When I go home on the weekends, there are at least three protests in my district. The protests are definitely in, and they are well attended with hundreds of thousands of people. And really the number one protection in our Constitution is the right to protest, freedom of speech, and then freedom of the press. So it is a very protected area, and this hearing is raising major concerns about the technology and the secrecy and the Privacy Act.

But before I start jumping on the FBI, I do have to share my appreciation. Three months ago, two bombs went off in the district that I'm privileged to represent. Many people were injured. Gratefully, no one was killed. But in 48 hours, the FBI and the police working together apprehended the person that was causing so much damage to innocent people. So I want to personally thank you, working 24 hours a day to crack down and catch.

So there's a conflict now. We live in probably the most dangerous time for innocent people because of attacks on so-called soft targets. And you've done a great job, but we've got to be careful about the transparency that you provide and protections. And it is essential that the FBI pursue its law enforcement agenda, as you do, but with transparency and with the protection of civil liberty and privacy as two of the most guiding principles.

Now, according to the GAO report, the FBI has been years behind in fulfilling its reporting obligations under the Privacy Act, the E–Government Act, and internal privacy policies for its facial recognition system. And as a result of the FBI's delay in complying with reporting these obligations, GAO found—and correct me if I am wrong, Ms. Maurer—and I quote, they said: "The public had limited understanding of the nature of the system and how their personal information, including face images, is being used and protected," end quote.

So I'd like to ask you, Ms. Maurer, what obligations did the FBI have to the public in this area?

Ms. MAURER. Thank you very much for the question. The FBI was obligated to provide transparency in how it was planning to use and eventually did start using the facial images of the members of the American public. There were a number of different reporting requirements that the FBI, through the Department of Justice, failed to meet.

They eventually did issue the required privacy notification documents. It was only years after they started using both of their sys-

tems for real-world use. That was of great concern to us from a transparency perspective.

Mrs. MALONEY. So, in other words, did the FBI meet its legal obligations with regard to updating and publishing these critical privacy documents that you mentioned?

Ms. MAURER. No. They did not.

Mrs. MALONEY. Now, can you explain what these privacy documents are? What are the Privacy Impact Assessments and the System of Records Notices? What is it?

Ms. MAURER. A Privacy Impact Assessment is required by the E–Gov Act. It's required of any Federal system when it's first created and when it is newly expanded. It is to provide transparency so the public has an understanding of how their personal information is being used.

The System of Records Notice is required under the Privacy Act. That's also when new systems are established. It pursues—tries to achieve a similar goal: transparency.

These are both useful documents. The PIAs, in particular, provide a fair bit of information and detail about how personal information is being used by the Federal Government. We thought it was important for them do it in a timely basis. They did not do so.

Mrs. MALONEY. Ms. Lynch is a representative of an organization that represents the public.

Why should the public be concerned about this? What's the impact of this?

Ms. LYNCH. I think the impact is that the public cannot assess what our government is doing if the government doesn't follow the law by producing Privacy Impact Assessments and updating the System of Records Notices.

So this has real impact on my job because I read through these things. And I write about them, and I try and tell people, including journalists and the public and our members, what's going on.

So, for example, I had no idea—and I think most privacy advocates had no idea—exactly how many images the FBI could access until the GAO published its report in 2016.

I think that most estimates were closer to about 50 million, and it turned out that the FBI could access about 412 million. So that's a significant difference, and if the Bureau is not responsible in publishing information on its divisions and on the impact of its programs, the public has no idea what's going on.

Mrs. MALONEY. Well, my time has expired, and thank you.

Mr. DUNCAN. Mr. Grothman, have you had a chance to catch your breath?

Mr. GROTHMAN. No, I haven't, but we'll charge ahead anyway without catching my breath.

Ms. Del Greco, do you think you have my face? Do you have access to the data regarding my face, do you think?

Ms. DEL GRECO. We would only access a face that you would have in a DMV record if there was an active FBI investigation or——

Mr. GROTHMAN. So you have it. If you had to, you could get it.

Ms. DEL GRECO. If you're one of the States that we have an MOU with.

Mr. GROTHMAN. Is Wisconsin one? Do you know off the top of your head? Maybe you don't know.

Ms. DEL GRECO. I'm not sure, sir.

Mr. GROTHMAN. Do you see why people are concerned about having the government have access to data in which you can tell where I am at any given time, given that we have more photos of people in the crowd, people in the stands, whatever? Do you see any concern as the government databases or access to databases, as you say, grows, grows, grows all the time?

Ms. DEL GRECO. Of course, I see why there would be a concern. However, we want to ensure the public that we are protecting their privacy by only accessing the data for legal purposes and a law enforcement purpose.

Mr. GROTHMAN. Do you think, in the past, the government's done a good job in making sure data is only accessed for legal purposes?

Ms. DEL GRECO. I do.

Mr. GROTHMAN. The IRS, for example?

Ms. DEL GRECO. I definitely do. Our FACE Services Unit will undergo an audit in accordance with the CJIS Audit Unit. And we also will audit the State and local agencies for their use of our system.

Mr. GROTHMAN. Does the FBI deploy real-time facial recognition technology on my video surveillance camera video feeds?

Ms. DEL GRECO. I'm not an expert in all areas of the FBI. In my area, we do not.

Mr. GROTHMAN. Would anybody else care to take a crack at that? Oh, okay.

Are you aware, is anybody aware of any domestic law enforcement entities that utilize or would ever plan to utilize real-time facial recognition technology?

Mr. BEDOYA. Yes, sir, if I may. We are. We're aware of six major law enforcement agencies that have either stated plans to use real-time face scanning or have actually purchased the technology or have said they are using it. So this is very much real. And about a quarter of the current body camera vendors are making provisions for use of face recognition off of body camera video. So this is very real.

Mr. GROTHMAN. Explain how that is going to work.

Mr. BEDOYA. It could work any number of ways. Probably the riskiest and most threatening way would be for every face that walks past a police officer to be scanned. So not just the faces of criminals, not just the faces of terrorists, the face of every man, woman, and child that walks by. To our knowledge, we've yet to see that, but we have seen it off of surveillance cameras.

Mr. GROTHMAN. But they have the ability to do it. It must be there for some purpose, right?

Mr. BEDOYA. A DOJ-funded study found that body camera vendors are, quote, "fine tuning" the ability to incorporate face recognition into body cameras. And I have a copy of that report, and I am happy to submit it to you on the record.

Mr. GROTHMAN. Would it be the type of thing where, eventually, if I'm walking by a cop, a police officer, it would show up that there is Glenn Grothman? If we're walking down the street?

Mr. BEDOYA. To our knowledge, right now, this operates on smaller watch lists, but the technology is getting better and better such that, eventually, in theory, it could encompass much larger databases like, for example, Wisconsin's driver's license database. To our knowledge, it does not operate on that large a database, but that is certainly where this appears to be headed.

Mr. GROTHMAN. Okay. So the day is going to come where Big Brother, if we call it that, will know, as we walk down the street, there's Ms. Del Greco and Ms. Maurer and Mr. Romine and just shows up that this is who is walking along or this is who I am seeing?

Mr. BEDOYA. Again, this is what a Department of Justice-funded study released at the end of last year said: fine-tuning face recognition capabilities for body cameras. To be clear, those capabilities don't necessarily need to be real-time right now. They could be after-the-fact face scanning, but certainly this is what a lot of law enforcement vendors are offering right now in terms of the surveillance cameras, and they want to go to the body camera——

Mr. GROTHMAN. Okay.

Mr. Hutchinson, where is this technology going?

Mr. HUTCHINSON. Yes, sir. Thank you. I wanted to comment. That technology is not commercially available right now. It is true that there is facial recognition technology available that can detect faces in video feeds. It has not been deployed to body-worn cameras. Also, as far as the access to the data——

Mr. GROTHMAN. Is it going to be?

Mr. HUTCHINSON. Potentially, potentially. It can be used with video feeds, but it's important to understand how the data is loaded into the camera so that it can be detected or identified. And as Mr. Bedoya stated, usually it is only watch list data, and as Ms. Del Greco stated, it is typically only felons. It typically does not have access to every single face imaginable.

Mr. GROTHMAN. Do you think some day it will? I could imagine why people would want it to.

Mr. HUTCHINSON. That would depend on the particular use case for the Federal law enforcement entity.

Mr. GROTHMAN. Can you explain why FRT is less accurate when used to identify certain groups of people?

Mr. HUTCHINSON. The algorithms are mathematic; they are math instructions for a computer basically. And they use certain vectors to determine how a face is searched and how it is identified in a database. It is highly dependent on the algorithm that you use. It is also highly dependent on the data in the database, but it is also dependent on the quality. And that's the most important piece. There have been some tests that indicate that certain groups of folks, whether its ethnicities or so forth, there can be challenges; the algorithms perform differently. But it is very important to understand what type of testing data is used to train that algorithm, because there was—I wanted to make a clarification earlier: a lot of the data the vendors use is not homogeneous. It is purposefully heterogeneous, and it has a lot of different faces from different races and different ages and different sexes, specifically to tune the data so that it does not have any sort of biases

Mr. DUNCAN. I'm sorry. We need to move on now to Ms. Kelly.

Ms. KELLY. Thank you, Mr. Chair.

The FBI's facial recognition systems include images from external partners such as the State Department, the Department of Defense, and at least 17 States. These external systems, however, operate, from my understanding, independently of the FBI's protocol and standards. And the GAO has raised concerns about that. According to the GAO, and I quote: "Because the FBI does not assess the accuracy of its partners' technology, it risks relying on technologies that could potentially have higher error rates or could be obsolete."

Ms. Del Greco, does the FBI do anything to ensure that the results it receives from the face recognition systems of its Federal and State law enforcement partners are accurate?

Ms. DEL GRECO. We do not have the authority to test external agency databases. Rather, we focus on the quality of the data that we're getting. So we share training tools. We offer training, and we share our best practices.

Ms. KELLY. Does the FBI do anything—I'll get to you—does the FBI do anything to make sure its Federal and State partners are taking adequate measures to protect against misuse of a system? And if you don't, why not?

Ms. DEL GRECO. We have a robust audit process at the FBI. We audit the State and local and Federal agencies. We have a sanctions process that's in place for noncompliance. There is a letter of censure that is issued if there is a misuse identified. If that is not corrected, we raise it to the level in the State to the Governor. If that is not corrected, and then we will shut off the system from the State.

Ms. KELLY. I see you want to say something.

Ms. MAURER. Yes, absolutely. We are happy that the FBI has begun to conduct these audits. I would note that they didn't start doing these audits or have these audits include facial recognition technology until after our report.

In terms of our recommendation to the FBI to assess the accuracy of the information that it receives from the other databases, our recommendation was not intended to require the FBI to independently assess the validity of other databases but, rather, have a better understanding of the accuracy for its own uses. The FBI has that technical capability. They can build it into the operational reviews. That was another one of our recommendations. So they can do it; they just chose not to.

Ms. KELLY. Any comment?

Ms. DEL GRECO. Well, we disagree. We have trained fingerprint—I'm sorry facial recognition examiners—they are called biometric image specialists—that go through rigorous training. So, when a candidate comes back, it's not a positive identification; it takes human review to find a most likely candidate.

Ms. KELLY. Thank you.

The FBI also claims that it does not have the authority to oversee its Federal and State partners, as you said, yet the FBI's Criminal Justice Information Services Unit enforces similar external audit policies for other programs. According to GAO, and again, I quote: "CJIS security policy states that the CJIS Audit Unit is required to conduct triannual audits of each of its States and local

law enforcement users to assess agency compliance with applicable statutes, regulations, and policies related to the CJIS systems."

Ms. Maurer, do these audits include face recognition searches of the FBI system?

Ms. MAURER. Recently, the FBI has begun to include facial recognition as part of these audits they are conducting of different States. To my understanding, I think they have completed four of those, but those were not begun until after our report was issued.

Ms. KELLY. And you fully support the idea—so they are done in only four States, or they've only done four?

Ms. MAURER. They've only done them in four States so far. They've told us they plan to do them in the others. These are parts of broader audits that the FBI does of how the States are using the full array of biometric information.

Ms. KELLY. Mr. Bedoya, did you have a comment?

Mr. BEDOYA. Ms. Kelly, I do. I just want to clarify what's being discussed here. We're talking about 36,000 searches of driver's license photos, including likely your face, since you're an Illinois driver. And none of those searches, per the GAO's reporting, were audited for misuse or abuse.

So, going forward, it sounds like there will be an audit, which is terrific. But since 2012, the FBI is saying there's going to be these audits, and only now this year—and that was before Congress, audits will be done before Congress. Only now this year are they starting to be done.

Ms. KELLY. Ms. Del Greco, when will you get to the other States?

Ms. DEL GRECO. So, during the GAO review, we had a paper that was going through our Advisory Policy Board to talk about the audits and how the audits would be conducted. It was intended to do the audits as part of our triannual audit process with the CJIS Audit Unit. We do intend to audit all State, local, Federal agencies, as well as the FBI FACE Services.

Ms. KELLY. Do you have a timeline?

Ms. DEL GRECO. The FBI FACE Services will be audited in 2018. There is a schedule for the other States.

Ms. KELLY. I am out of time. So I yield back.

Mr. DUNCAN. Thank you very much.

Mr. Clay.

Mr. CLAY. Thank you, Mr. Chair.

And let me thank the panel of witnesses.

Let me state in the beginning that misidentifying a criminal suspect can have dramatic and permanent real-world implications. So, with that, last year, the GAO released a report on its review of the FBI's use of facial recognition technology. Chief among GAO's findings is that the FBI has not examined how often, and I quote, "face recognition searches erroneously match a person to the database," in other words, the false positive rate.

Dr. Romine, why is testing for false positives so important in assessing the accuracy of a facial recognition system?

Mr. ROMINE. When we test algorithms for accuracy, one of the characteristics we want to know is not just how often an image that is in the gallery that matches a probe is returned but also the extent to which the algorithm can fail to recognize or, in some cases, return erroneous results, as you mentioned. And that's just

an important consideration with regard to measurements, science, capabilities. We want to be sure that we provide as much information to stakeholders as we can about all aspects of the performance of the algorithms that we test.

Mr. CLAY. I see. And to better address the challenge of false positive matches, GAO's report recommends that the FBI begin testing the false positive rate.

Ms. Del Greco, despite GAO's findings and recommendation as to the importance of testing the false positive rate, the FBI did not agree with GAO's recommendation. Is that right?

Ms. DEL GRECO. That is correct, sir. A false positive rate measures when searches are resulting in one match, and we always receive the candidate list back that requires a human review.

Mr. CLAY. But aren't you concerned that, by not adopting this testing, the FBI may be using a system that isn't as accurate as it should be?

Ms. DEL GRECO. The false positive rate is not based on the return of the candidates but of the human reviewing and the response that the human review gives to either the examiner or FBI agent.

Mr. CLAY. So what happens when you bring a suspect in and it's the wrong one? Do you recognize that fault, or do you go on what your facial recognition?

Ms. DEL GRECO. We provide a most likely candidate to the FBI agent. The FBI agent then has to make the determination if that is the person that they are—that is under investigation.

Mr. CLAY. Well, that sounds like a crapshoot. It sounds like you're taking a chance: maybe this guy is the one. I mean, come on.

Ms. DEL GRECO. Our system doesn't provide positive identification for facial recognition.

Mr. CLAY. Okay.

Ms. Maurer, can you explain how the adoption of such testing could improve the accuracy of the FBI system?

Ms. MAURER. Sure. First off, as my colleague from NIST has correctly pointed out, false positive testing is a bedrock of accuracy for facial recognition technologies, which is the reason why we recommended the FBI do that.

Our understanding is their system has a technical capability to test for false positives. They chose not to exercise that capability.

We are also concerned about the way it could impact people in the real world as well as the impact on the FBI's use of its own resources. They could end up spending some of their valuable investigative time on wild-goose chases rather than focusing on the actual individual they are trying to find.

Mr. CLAY. Yeah. It sounds like a crapshoot to me. It sounds like you're just shooting in the dark, maybe this is the guy.

You know, Ms. Del Greco, in your written testimony, you state that the FBI's facial recognition system, and I quote, "is only used as an investigative lead and not as a means of positive identification." Is that right?

Ms. DEL GRECO. That is correct, sir.

Mr. CLAY. Ms. Lynch, if the FBI says facial recognition searches are only used as investigative leads, can you explain the con-

sequences for potentially innocent individuals who are identified due to a false positive result?

Ms. LYNCH. Well, if investigative leads are returned, that means that a number of people will be returned and produced as suspects for a crime. Each one of those people could be brought in for questioning. Each one of those people will have to justify where they were on a given time and day. It's very difficult, I think, for a lot of people to prove where they were in the past. And it makes people suspects for crimes that they didn't commit.

Mr. CLAY. My time is up, but I'm sure it wreaks havoc on peoples' lives.

So thank you, Mr. Chairman.

Mr. DUNCAN. Ms. Del Greco, the Bureau presently has memorandums of understanding with 18 States in regard to this facial recognition program. Do you know, are other States going to be added in the future, or is there an effort being done in that regard now to move this to all 50 States?

Ms. DEL GRECO. Where there's a law that allows the use of the DMV photos for law enforcement purposes, we will continue to work with those States to develop an MOU. There are States that do not allow the use of facial recognition technology. Not all 50 States will have MOUs with the FBI.

Mr. DUNCAN. All right.

Ms. Lynch, do you have any concerns about using photographs to identify people's fingerprints—identifying fingerprints from photos?

Ms. LYNCH. Identifying fingerprints or identifying faces? I think the big difference between fingerprints and face images is that generally somebody knows if they are providing that fingerprint. So, to obtain a fingerprint from somebody, in general——

Mr. DUNCAN. No. I mean, if they have a photo of a person with an open palm, using that photo to identify, to take the fingerprints from that photo.

Ms. LYNCH. I'm not sure I——

Mr. DUNCAN. You haven't heard of that?

Ms. LYNCH. Well, palm prints are——

Mr. DUNCAN. Mr. Bedoya, I think, knows something about it.

Mr. BEDOYA. It's a series of little-known studies; Dr. Latanya Sweeney, among others, has shown you can, in fact, do that. So this was done famously in Germany. Some individuals took a German Minister's photo of his hand and actually figured out his fingerprint from that. So that is something that is technically possible now but, to my knowledge, is not in wide use in the United States. But that's—it may be in use; I just don't know it.

Mr. DUNCAN. All right.

Well, I want to thank all the witnesses for taking the time to appear here today.

And I ask unanimous consent that members have 5 legislative days to submit questions for the record.

Without objection, so ordered.

If there's no further business, the committee stands adjourned.

[Whereupon, at 11:37 a.m., the committee was adjourned.

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

June 23, 2016

Senator Chuck Grassley, Chairman
Committee on the Judiciary
437 Russell Senate Office Building
Washington, DC 20510

Senator Patrick J. Leahy, Ranking Member
Committee of the Judiciary
437 Russell Senate Office Building
Washington, DC 20510

Congressman Bob Goodlatte, Chairman
Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515

Congressman John Conyers, Ranking Member
Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515

Congressman Jason Chaffetz, Chairman
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, DC 20515

Congressman Elijah Cummings, Ranking Member
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, DC 20515

Re: The FBI's Use of Facial Recognition and Proposal to Exempt the Bureau's Next Generation Identification Database from Privacy Act Obligations

Dear Senators Grassley and Leahy and Representatives Goodlatte, Chaffetz, Conyers, and Cummings:

Thank you for your continued oversight of the Federal Bureau of Investigation ("FBI") programs that impact the privacy, civil liberties, and human rights of Americans and lawful permanent residents. Oversight hearings promote transparency and accountability and help ensure that the FBI fulfills its mission while upholding American values and constitutional freedoms.

We, the undersigned privacy, transparency, civil rights, human rights, and immigrant rights organizations, write today to bring your attention to the FBI's recent proposal to exempt the Bureau's massive biometric database known as Next Generation Identification ("NGI") from the protections provided by the Privacy Act of 1974, and the FBI's extensive use of facial recognition technology without proper oversight. We urge you to hold an oversight hearing on the NGI program and the FBI's use of biometric data.

NGI is a massive biometric database that was launched in 2008 and went fully operational in Fall 2014.[1] The database contains the biometric data on millions of US citizens

[1] FBI Press Release, *FBI Announces Full Operational Capability of the Next Generation Identification System* (Sept. 15, 2014), https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-full-operational-capability-of-the-next-generation-identification-system.

and immigrants.[2] NGI incorporates numerous biometrics including fingerprints, facial recognition, and iris recognition.[3] The database contains profiles on arrestees and people with records as well as individuals with no connection to the criminal justice system, and NGI is used for both law enforcement and non-law enforcement purposes.[4] Through NGI's Interstate Photo System ("NGI-IPS"), the FBI runs a face recognition service with over 30 million photos from 16.9 million individuals that is accessed by various state and local law enforcement agencies.[5]

Additionally, the FBI has agreements with 16 states to request facial recognition searches of state repositories of photos consisting mostly of driver license photos.[6] From 2011 to 2015, the FBI ran over 36,000 facial recognition searches of *well over 170 million driver's license photos* – photos of law-abiding drivers unconnected to the criminal justice system.[7] The FBI is currently negotiating with 18 other states to include their driver's license photos in these searches.[8] All of these searches have been conducted without any judicial oversight or internal audits.

Per the Systems of Record Notice, NGI will collect personal information, including biometric data, for the purposes of employment, licensing, military service, volunteer service, background checks, immigration benefits, lawful detention, criminal inquiries, or civil law violations, and through sharing agreements with foreign countries or international organizations.[9] The default retention of these records is until the individual turns 110 years old or seven years after the FBI has been notified of the individual's death regardless of whether the original purpose for the collection has come to an end or not.[10]

The FBI is unnecessarily retaining vast amounts of personal and biometric information and exposing millions of people to a potential data breach. In light of the increasing number of data breaches, and in particular the Office of Personnel Management's data breach, there is no excuse for unnecessarily retaining personal information on millions of people. Biometric data cannot be changed if it is compromised. The collecting of biometric data raises numerous

---

[2] FBI, *Next Generation Identification (NGI) Monthly Fact Sheet* (Dec. 2015), https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/december-2015-ngi-fact-sheet.pdf.
[3] FBI, *Next Generation Identification*, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi.
[4] *See Id.*
[5] GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, 10 (May 2016).
[6] *Id.* at 50. The FBI also recently ran a pilot to run facial recognition searches on the vast repository of passport photos maintained by the State Department. GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, 48 (May 2016).
[7] *Id.* at 47-49.
[8] *Id.* at 50.
[9] Notice of Privacy Act System of Records, 81 Fed. Reg. 27284, 27284-85 (May 5, 2016) (Notice of Privacy Act System of Records modified extension, 81 Fed. Reg. 36350 (June 6, 2016)).
[10] *See* Privacy Impact Assessment for the Next Generation Identification (NGI) Interstate Photo System, § 3.4 (Sept. 15, 2015), https://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system; *see also* Privacy Impact Assessment Next Generation Identification (NGI) – Retention and Searching of Noncriminal Justice Fingerprint Submissions, § 3.4 (Feb. 20, 2015).

privacy and civil liberties issues. For many communities, it also raises serious religious concerns.[11]

The collection of biometric data on millions of people gives law enforcement the ability to identify individuals without probable cause, reasonable suspicion, or any other legal standard that might otherwise be required for law enforcement to obtain traditional identification. Through the use of biometric identifiers like facial recognition, law enforcement can covertly and remotely identify people on a mass scale.

The FBI has a unit dedicated to the use of facial recognition. The Facial Analysis, Comparison, and Evaluation ("FACE") Services Unit "receives facial probe images from the field, conducts a face search of all available facial recognition (FR) systems, and provides results back to the requesting agent."[12] Furthermore the FBI's Biometric Center of Excellence continues to explore "the use of new and enhanced biometric technologies and capabilities for integration into operations"[13] with minimal transparency.

The FBI's use of facial recognition through NGI and its FACE Services Unit lacks proper public oversight. A recent GAO report determined that the "FBI has not completed audits to oversee the use of NGI-IPS or FACE services."[14] The GAO report concluded that "without conducting audits to determine whether users are conducting face image searches in accordance with CJIS policy requirements, FBI officials cannot be sure they are implementing face recognition capabilities in a manner that protects individuals' privacy."[15] Furthermore, the FBI has failed to timely update the public through Privacy Impact Assessments required by law.[16] These privacy assessments are essential to informing the public on how the FBI mitigates the privacy risks associated with its information systems.[17]

Congress often holds oversight hearings of the FBI, but more often than not the FBI's NGI database and its use of biometrics receives too little scrutiny. The last time NGI and specifically the FBI's use of face recognition were a predominant focus of a congressional hearing was in July 2012 before the Senate Judiciary subcommittee on Privacy, Technology and

---

[11] Many individuals have significant religious objections to the collection, retention, and/or sharing of their biometric data.

[12] Standard Operating Manual: Facial Analysis, Comparison, and Evaluation (FACE) Service Unit (Version 1.0 Apr. 9, 2013), https://epic.org/foia/fbi/faces/FBI-SOP-FACES-Unit.pdf.

[13] FBI, *Biometric Center of Excellence*, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/.

[14] GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, 23 (May 2016), http://www.gao.gov/assets/680/677098.pdf.

[15] *Id.* at 33.

[16] *Id.* at 18-19.

[17] *See* DOJ Office of Privacy and Civil Liberties, *Privacy Impact Assessments: Official Guidance*, 4 (Revised July 2015), https://www.justice.gov/opcl/file/631431/download.

the Law.[18] In his statement for the record, Senator Franken expressed the risks of the use of facial recognition by the FBI without proper oversight, stating:

> I fear that the FBI pilot could be abused to not only identify protestors at political events and rallies, but to target them for selective jailing and prosecution, stifling their First Amendment rights . . . . I also fear that without further protections, facial recognition technology could be used on unsuspecting civilians innocent of any crime—invading their privacy and exposing them to potential false identifications.[19]

The risks of NGI and the large-scale collection, use, retention, and sharing of biometrics are well understood by the privacy and civil liberties community. Because of these risks, public interest organizations have repeatedly called for the review of NGI.[20] In 2011, 70 organizations urged the Inspector General of the Department of Justice to investigate the privacy and civil liberties implications of the FBI's NGI program.[21] In 2014, as NGI neared full operational capacity, a coalition of civil liberties groups urged Attorney General Eric Holder to review the NGI program and release an updated Privacy Impact Assessment as a first step to robust review of the program.[22] Since that letter, NGI has gone fully operational with minimal oversight.

Most recently a coalition of public interest organizations called upon the Department of Justice to extend the public comment period for the FBI's proposal to exempt NGI from many of the most important protections provided by the Privacy Act of 1974.[23] The letter urged more time to "allow the public the opportunity for a careful, step-by-step examination of both the NGI System of Records Notice and the FBI's proposal to render that system largely secret."[24]

In a public interest case against the FBI, U.S. District Judge Tanya Chutkan stated, "There can be little dispute that the general public has a genuine tangible interest in a system

---

[18] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 112th Cong. (2012).
[19] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 112th Cong. 2 (2012) (statement for the record of Senator Al Franken).
[20] EPIC previously called for a congressional hearing on FBI's NGI database. Letter from EPIC to Senators Chuck Grassley and Patrick Leahy (Jan. 9, 2015), https://epic.org/foia/fbi/ngi/EPIC-to-SJC-re-NGI.pdf.
[21] Letter from Coalition of Civil Liberties groups to Cynthia A. Schnedar, DOJ Acting Inspector General (Sept. 11, 2011), https://epic.org/privacy/secure_communities/DOJ-S-Comm-Letter.pdf.
[22] Letter from Coalition of Civil Liberties groups to Eric Holder, U.S. Attorney General (June 24, 2014), https://www.privacycoalition.org/Ltr-to-Review-FBI-NGI-Program.pdf.
[23] Letter from Coalition of Civil Liberties groups to Erika Brown Lee, DOJ Chief Privacy and Civil Liberties Officer (May 27, 2016), https://epic.org/privacy/fbi/coalition-letter-urges-public-comment-extension-on-NGI.pdf.
[24] *Id.*

designed to store and manipulate significant quantities of its own biometric data, particularly given the great numbers of people from whom such data will be gathered."[25]

We urge the Committees to take up this issue as soon as possible and hold oversight hearings to assess the privacy, civil liberties, and human right issues raised by the FBI's massive biometric database and the Bureau's use of facial recognition technologies to search its own database, other federal department databases, and databases of state driver's license photos. We also urge the committees to require the FBI's compliance with the Privacy Act of 1974 and ensure ongoing public reports on the FBI's use, collection, retention, and disclosure of biometric data.

Sincerely,

18MillionRising.org
Advocacy for Principled Action in Government
American-Arab Anti-Discrimination Committee
American Civil Liberties Union
American Library Association
Amnesty International USA
Arab American Institute
Asian Americans Advancing Justice - Asian Law Caucus
Bill of Rights Defense Committee/Defending Dissent Foundation
Center for Democracy & Technology
Center for Digital Democracy
Center for Financial Privacy and Human Rights
Center for Media Justice
Center on Privacy & Technology at Georgetown Law
ColorOfChange.org
Constitutional Alliance
The Constitution Project
Consumer Action
Consumer Watchdog
Council on American-Islamic Relations
Cyber Privacy Project
Demand Progress
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Fight for the Future
Free Press Action Fund
Freedom of the Press Foundation
Government Accountability Project

[25] *EPIC v. FBI*, 72 F. Supp. 3d 338, 346 (D.D.C. Nov. 5, 2014). The case was a Freedom of Information Act lawsuit against the FBI for records about the Bureau's NGI database.

Immigrant Legal Resource Center
Media Mobilizing Project
MPower Change
National Association of Criminal Defense Lawyers
National Consumers League
National Day Laborer Organizing Network
National Employment Law Project
National Immigration Law Center
National Immigration Project of the National Lawyers Guild
National LGBTQ Task Force Action Fund
New America's Open Technology Institute
OpenTheGovernment.org
Patient Privacy Rights
Privacy Rights Clearinghouse
Privacy Times
Restore the Fourth
Sunlight Foundation
World Privacy Forum

JASON CHAFFETZ, UTAH
CHAIRMAN

ONE HUNDRED FOURTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225-5074
MINORITY (202) 225-5051
http://oversight.house.gov

September 6, 2016

The Honorable James B. Comey
Director
Federal Bureau of Investigation
950 Pennsylvania Avenue NW
Washington, D.C. 20535

Dear Director Comey:

The Federal Bureau of Investigation recently asked to exempt its Next Generation Identification (NGI) system from certain Privacy Act requirements.[1] Media reports and privacy advocates have raised questions about the scope of the NGI and the effect these exemptions would have on an individual's right to know whether the FBI possesses his or her biometric information, to request the information be removed, or to correct any inaccuracies within NGI.[2]

The NGI system is a database of biometrics, including fingerprints, palm prints, facial recognition, and a pilot program for iris recognition.[3] In addition to information from criminal matters, the FBI receives biometric information, including fingerprints and photographs, from individuals undergoing background checks for various purposes, including employment and licensing. Under the previous database, most of the fingerprints received for a non-criminal matter were destroyed by the FBI after processing.[4] With the NGI, however, the FBI will retain these non-criminal fingerprints and add them to a single searchable database consisting of all fingerprints submitted to the FBI.[5] These non-criminal fingerprints will only be removed at the request of the submitting agency or by court order.[6]

---

[1] U.S. Dep't of Justice, *Privacy Act of 1974; Implementation,* 81 Fed. Reg. 27288 (May 5, 2016) (Notice of proposed rulemaking).

[2] Gabe Rottman, *Massive FBI Biometric Database Must be Subject to Appropriate Public Scrutiny*, Center for Democracy and Technology, May 31, 2016, *available at* https://cdt.org/blog/massive-fbi-biometric-database-must-be-subject-to-appropriate-public-scrutiny/; *see also,* Joshua Eaton, *Tech Civil Liberties Leaders Fight FBI Biometric Program*, CHRISTIAN SCIENCE MONITOR, June 1, 2016.

[3] Federal Bureau of Investigation, Next Generation Identification, *available at* https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi.

[4] Federal Bureau of Investigation, Privacy Act Assessment Next Generation Identification – Retention and Searching of Noncriminal Justice Fingerprint Submissions, *available at* https://www.fbi.gov/foia/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions.

[5] *Id.*

[6] *Id.*

The large scale recording, retention, and use of biometric information by law enforcement raises serious privacy concerns. Privacy groups, civil liberty advocates, and private citizens alike have requested additional time to submit comments regarding the FBI's proposed exemption to the Privacy Act.[7] A recent GAO analysis of the NGI's Interstate Photo System (NGI-IPS) also found the FBI should better ensure the privacy and accuracy of its facial recognition technology systems.[8] There have also been troubling concerns about the potential for racial bias in the recognition software.[9] The Committee is interested in learning about the NGI, the NGI-IPS, and the effect of any exemptions to the Privacy Act being considered.

To assist the Committee, please provide the following documents and information as soon as possible, but by no later than 5:00 p.m. on September 20, 2016:

1. All policies, guidance, or memoranda on the use of facial recognition technology, including, but not limited to, internal FBI guidance and guidance or memoranda provided by the FBI to state and local entities;

2. All policies, guidance, or memoranda on the use and retention of images and data collected when using facial recognition technology;

3. Documents referring or relating to the accuracy rate and error rate for the facial recognition technology being used by the FBI and the methodology used to arrive at these rates, including, but not limited to, the source of the rate and the results of any testing the FBI has performed on its facial recognition technology;

4. All memoranda of understanding or non-disclosure agreements with state and local law enforcement agencies regarding the use of the FBI's facial recognition technology or the use of information obtained through the use of facial recognition technology;

5. Documents referring or relating to any allegations regarding potential misuse of the FBI's facial recognition technology;

6. Documents sufficient to show the number of photographs (from any source) contained in the NGI; and

7. Documents sufficient to identify the source of each photograph contained in the NGI.

---

[7] *See* Letter from a coalition of civil rights, human rights, immigrant rights, privacy, and transparency organizations and companies to Ms. Erika Brown Lee, Privacy Analyst, Privacy & Civil Liberties Office, U.S. Dep't of Justice (May 27, 2016), *available at* https://www.eff.org/document/2016-letter-fbi-re-NGI.

[8] Gov't Accountability Office, *Facial Recognition Technology: FBI Should Better Ensure Privacy and Accuracy* (May 2016) (GAO-16-267).

[9] *Facial-Recognition Software Might Have a Racial Bias Problem*, The Atlantic (Apr. 7, 2016) (online at http://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/).

The Committee on Oversight and Government Reform is the principal investigative committee in the House of Representatives. Pursuant to House Rule X, the Committee has authority to investigate "any matter" at "any time."

When producing documents to the Committee, please deliver production sets to the Majority staff in Room 2157 of the Rayburn House Office Building and the Minority staff in Room 2471 of the Rayburn House Office Building. The Committee prefers, if possible, to receive all documents in electronic format. An attachment to this letter provides additional information about responding to the Committee's request.

Please contact Sean Brebbia of the Majority staff at (202) 225-5074 with any questions about this request. Thank you for your attention to this important matter.

Sincerely,

Jason Chaffetz
Chairman

Elijah E. Cummings
Ranking Member

Enclosure

Questions for Mr. Chuck Romine
Director of Information Technology Laboratory
National Institute of Standards and Technology

Questions from Chairman Jason Chaffetz

March 22, 2017, Hearing: "Law Enforcement's Use of Facial Recognition Technology"

---

1. The FBI has reportedly failed to test its facial recognition technology (FRT) for false positives. Please provide a list and description of NIST's recommended methods for testing FRT accuracy and the relevance of false positive rates to the accuracy of facial recognition technology.

    a. How often should a FRT system be tested for accuracy? Can the accuracy rate change over time?

    NIST Response:
    Once an algorithm is deployed, its accuracy will not change unless:
    1) its configuration parameters change, for example, due to a system or software upgrade;
    2) the photographic or demographic properties of images passed to the algorithm change, for example, due to a significant change in demographics; or
    3) the number of images enrolled in the database changes significantly.

    New testing should be conducted if any of the above changes for a deployed FRT.

    Facial recognition is an active area of research, and algorithms are constantly improving. If the puporse of testing is to benchmark the state-of-the-art, industry testing should be conducted on a regular schedule in line with development schedules, while considering other factors such as cost and mission needs.

2. A report by NIST discussed the "other race effect" - the tendency for algorithms to be more accurate at identifying people of the same race that developed the algorithm and less accurate at identifying the face of other races. Other studies have suggested FRT may perform less accurately on certain demographics, to include darker skin, younger people and women.

    a. Is there an established method for determining if an algorithm displays "the other race effect"?

    NIST Response:
    There is currently no established method, although a standardized method is under development within the Biometrics subcommittee of the International Organization for Standardization.

    b. Is FRT less accurate for certain demographics? If so which demographics? In what ways is it less accurate?

    NIST Response:
    NIST testing revealed that accuracy of facial recognition technologies is influenced by demographics. Tests using visa photographs showed that false positive rates were generally lower in white populations, and higher in East Asian, South Asian, and African populations, and

that false positive rates are generally lower in men than women. Age also matters, where accuracy declines for younger populations. In a one-to-many search, NIST would expect a system to produce more candidates of the same race as the probe image, if those populations were prevalent in the database, and particularly if the probe image was a woman, or from East Asia, South Asia or Africa.

False negative rates are also affected by demographics, though to a lesser extent. Tests using mugshot photos showed that false negative rates were generally lower for men than women. Face images with dark skin gave lower false negative rates than lighter skin. Finally, false negative rates increase with the age of subjects.

c. Is there an established method for determining whether an algorithm demonstrates the "other race effect"?

NIST Response:
Please see response to question 2a above.

d. What are the solutions for improving FRT's accuracy among the demographics for which it is less accurate?

NIST Response:
FRT dependence on demographic can generally be improved by:
1) improving the photographic capture process, to ensure high quality capture and excellent conformance to published capture standards,
2) establishing a test procedure and metrics for quantifying demographic effects,
3) challenging developers to use those metrics to improve their systems, and
4) selecting systems with algorithms that have been demonstrated to exhibit minimal sensitivity to demographics.

3. Has NIST tested the exact algorithm being used by the FBI?

NIST Response:
NIST tested a late-2012 edition of the operational NGI algorithm. The NIST test was limited to measurement of one-to-many identification accuracy in databases with sizes up 1.6 million subjects. NIST sent a report to the FBI in January 2015 detailing the measurement methodology and the results.

4. Has NIST made any efforts at testing the FRT used by the FBI? What was the FBI's response to NIST's efforts to test the FBI's FRT software?

NIST Response:
Both NIST's 2010 and 2013 open FRT testing campaigns evaluated algorithms from a number of vendors, including several algorithms from the supplier that FBI ultimately selected for NGI deployment. Later, in 2014, NIST tested a 2012 implemetation of the NGI algorithm.. NIST performed a comparative analysis of its accuracy with that of five 2013 prototypes from the NGI algorithm supplier. NIST sent a report to FBI in January 2015 detailing the measurement methodology and the results.

5. Of the algorithms NIST was able to test, which is the most similar to the FBI's? Please include information as to in what ways they are similar.

NIST Response:
In its test campaign in 2010, NIST measured accuracy of algorithms from multiple vendors, including the supplier of the NGI algorithm. The results of that test were provided to the FBI's prime contractor for NGI to inform their trade study. In its next test campaign, in 2013, NIST tested five new algorithm prototypes from the NGI developer. This allowed NIST to tabulate accuracy of the 2013 variants alongside that measured for a late 2012 copy of operational NGI algorithm. In May 2014, NIST reported on the accuracy of five variants of algoirthms from the same manufacturer as that used within NGI. The prototypes that NIST evaluated were submitted by the vendor's research laboratory. NIST has no information on which prototype most closely aligns with the deployed NGI variant or how they differ from each other.

○