

FACIAL RECOGNITION TECHNOLOGY: EXAMINING ITS USE BY LAW ENFORCEMENT

HEARING BEFORE THE SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY OF THE COMMITTEE ON THE JUDICIARY U.S. HOUSE OF REPRESENTATIVES ONE HUNDRED SEVENTEENTH CONGRESS FIRST SESSION

TUESDAY, JULY 13, 2021

Serial No. 117-33

Printed for the use of the Committee on the Judiciary



Available via: <http://judiciary.house.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2022

COMMITTEE ON THE JUDICIARY

JERROLD NADLER, New York, *Chair*
MADELEINE DEAN, Pennsylvania, *Vice-Chair*

ZOE LOFGREN, California	JIM JORDAN, Ohio, <i>Ranking Member</i>
SHEILA JACKSON LEE, Texas	STEVE CHABOT, Ohio
STEVE COHEN, Tennessee	LOUIE GOHMERT, Texas
HENRY C. "HANK" JOHNSON, JR., Georgia	DARRELL ISSA, California
THEODORE E. DEUTCH, Florida	KEN BUCK, Colorado
KAREN BASS, California	MATT GAETZ, Florida
HAKEEM S. JEFFRIES, New York	MIKE JOHNSON, Louisiana
DAVID N. CICILLINE, Rhode Island	ANDY BIGGS, Arizona
ERIC SWALWELL, California	TOM McCLINTOCK, California
TED LIEU, California	W. GREG STEUBE, Florida
JAMIE RASKIN, Maryland	TOM TIFFANY, Wisconsin
PRAMILA JAYAPAL, Washington	THOMAS MASSIE, Kentucky
VAL BUTLER DEMINGS, Florida	CHIP ROY, Texas
J. LUIS CORREA, California	DAN BISHOP, North Carolina
MARY GAY SCANLON, Pennsylvania	MICHELLE FISCHBACH, Minnesota
SYLVIA R. GARCIA, Texas	VICTORIA SPARTZ, Indiana
JOE NEGUSE, Colorado	SCOTT FITZGERALD, Wisconsin
LUCY McBATH, Georgia	CLIFF BENTZ, Oregon
GREG STANTON, Arizona	BURGESS OWENS, Utah
VERONICA ESCOBAR, Texas	
MONDAIRE JONES, New York	
DEBORAH ROSS, North Carolina	
CORI BUSH, Missouri	

PERRY APELBAUM, *Majority Staff Director & Chief Counsel*
CHRISTOPHER HIXON, *Minority Staff Director*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

SHEILA JACKSON LEE, Texas, *Chair*
CORI BUSH, Missouri, *Vice-Chair*

KAREN BASS, California	ANDY BIGGS, Arizona, <i>Ranking Member</i>
VAL DEMINGS, Florida	STEVE CHABOT, Ohio
LUCY McBATH, Georgia	LOUIE GOHMERT, Texas
MADELEINE DEAN, Pennsylvania	W. GREGORY STEUBE, Florida
MARY GAY SCANLON, Pennsylvania	TOM TIFFANY, Wisconsin
DAVID CICILLINE, Rhode Island	THOMAS MASSIE, Kentucky
TED LIEU, California	VICTORIA SPARTZ, Indiana
LOU CORREA, California	SCOTT FITZGERALD, Wisconsin
VERONICA ESCOBAR, Texas	BURGESS OWENS, Utah
STEVE COHEN, Tennessee	

JOE GRAUPENSPERGER, *Chief Counsel*
JASON CERVENAK, *Minority Counsel*

C O N T E N T S

TUESDAY, JULY 13, 2021

	Page
OPENING STATEMENTS	
The Honorable Sheila Jackson Lee, Chair of the Subcommittee on Crime, Terrorism, and Homeland Security from the State of Texas	1
The Honorable Andy Biggs, Ranking Member of the Subcommittee on Crime, Terrorism, and Homeland Security from the State of Arizona	4
The Honorable Jerrold Nadler, Chair of the Committee on the Judiciary from the State of New York	24
The Honorable Jim Jordan, Ranking Member of the Committee on the Judiciary from the State of Ohio	25
WITNESSES	
Gretta L. Goodwin, Director, Homeland Security and Justice, U.S. Government Accountability Office	28
Oral Testimony	31
Prepared Testimony	31
Barry Friedman, Jacob D. Fuchsberg Professor of Law and Faculty Director, Policing Project, New York University School of Law	49
Oral Testimony	51
Prepared Testimony	51
Robert Williams, Farmington Hills, Michigan	64
Oral Testimony	64
Prepared Testimony	66
Bertram Lee Jr., Media and Tech Policy Counsel, The Leadership Conference on Civil and Human Rights	71
Oral Testimony	71
Prepared Testimony	73
Kara Frederick, Research Fellow, Center for Technology Policy, The Heritage Foundation	80
Oral Testimony	82
Prepared Testimony	82
Jennifer E. Laurin, The Wright C. Morrow Professor of Law, The University of Texas at Austin School of Law	89
Oral Testimony	91
Prepared Testimony	91
Brett Tolman, Executive Director, Right on Crime	94
Oral Testimony	94
Prepared Testimony	96
Cedric L. Alexander, Former Public Safety Director, Dekalb County, Georgia and Former Member of President Obama’s Task Force on 21st Century Policing	100
Oral Testimony	100
Prepared Testimony	102

IV

LETTERS, STATEMENTS, ETC. SUBMITTED FOR THE HEARING	Page
Materials submitted by the Honorable Andy Biggs, Ranking Member of the Subcommittee on Crime, Terrorism, and Homeland Security from the State of Arizona, for the record	
A letter from Matthew Feeney, Director, Project on Emerging Technologies, Cato Institute, July 12, 2021	8
An article entitled, "Capitol Police to use Army surveillance gear to monitor Americans and 'identify emerging threats,'" American Military News	12
An article entitled, "Did agents raid home of wrong woman over Jan. 6 riot? Maybe," AP News	14
An article entitled, "Search warrant reveals why the FBI raided an Alaska couple's home," Alaska's News Source	18
An article entitled, "Homer residents said home was searched by FBI in connection to the Jan. 6 Capitol riots," Homer News	21
Materials submitted by the Honorable Jerrold Nadler, Chair of the Committee on the Judiciary from the State of New York, for the record	
A document entitled, "Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology," June 3, 2021	114
A letter from Don Erickson, CEO, Security Industry Association, July 13, 2021	123
A statement from Tawana Petty, National Organizing Director, Data for Black Lives	125
A statement from the Electronic Frontier Foundation	129
A statement from the Project on Government Oversight	132
Materials submitted by the Honorable Sheila Jackson Lee, Chair of the Subcommittee on Crime, Terrorism, and Homeland Security from the State of Texas, for the record	
A report entitled, "Facial Recognition Technology: Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees," United States Government Accountability Office	168
An article entitled, "The Problem of Bias in Facial Recognition," Center for Strategic and International Studies	194
An article entitled, "How America's surveillance networks helped the FBI catch the Capitol mob," The Washington Post	200
An article entitled, "Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use," The Washington Post	208

APPENDIX

Materials submitted by the Honorable Sheila Jackson Lee, Chair of the Subcommittee on Crime, Terrorism, and Homeland Security from the State of Texas, for the record	
A letter from Rashad Robinson, President, Color Of Change, July 16, 2021 ..	214
A letter from the NAACP Legal Defense and Educational Fund, Inc., July 20, 2021	221

QUESTIONS AND RESPONSES FOR THE RECORD

Questions for Gretta L. Goodwin, Brett Tolman, and Kara Frederick, submitted by the Honorable Louie Gohmert, a Member of the Subcommittee on Crime, Terrorism, and Homeland Security from the State of Texas, for the record	236
Answers from Gretta L. Goodwin, submitted by the Honorable Louie Gohmert, a Member of the Subcommittee on Crime, Terrorism, and Homeland Security from the State of Texas, for the record	239
Answers from Brett Tolman, submitted by the Honorable Louie Gohmert, a Member of the Subcommittee on Crime, Terrorism, and Homeland Security from the State of Texas, for the record	242
Answers from Kara Frederick, submitted by the Honorable Louie Gohmert, a Member of the Subcommittee on Crime, Terrorism, and Homeland Security from the State of Texas, for the record	244

FACIAL RECOGNITION TECHNOLOGY: EXAMINING ITS USE BY LAW ENFORCEMENT

Tuesday, July 13, 2021

HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

COMMITTEE ON THE JUDICIARY

Washington, DC

The Subcommittee met, pursuant to call, at 10:01 a.m., via Zoom, Hon. Sheila Jackson Lee [Chair of the Subcommittee] presiding.

Present: Representatives Jackson Lee, Nadler, Bass, Demings, McBath, Dean, Scanlon, Cicilline, Lieu, Correa, Cohen, Biggs, Jordan, Chabot, Gohmert, Steube, Tiffany, Massie, Fitzgerald, and Owens.

Staff Present: Arya Hariharan, Chief Oversight Counsel; John Doty, Senior Advisor; Moh Sharma, Director of Member Services & Outreach and Policy Advisor; Jacqui Kappler, Oversight Counsel; Priyanka Mara, Professional Staff Member and Legislative Aide; Cierra Fontenot, Chief Clerk; Atarah McCoy, Staff Assistant; Gabriel Barnett, Staff Assistant; Merrick Nelson, Digital Director; Kayla Hamed, Deputy Communications Director; Ben Hernandez-Stern, Counsel, Subcommittee on Crime, Terrorism, and Homeland Security; Ken David, Minority Counsel; Jason Cervenak, Minority Chief Counsel for Crime; and Kiley Bidelman, Minority Clerk.

Ms. JACKSON LEE. The Subcommittee will come to order. Without objection, the Chair is authorized to declare recesses of the Subcommittee at any time.

We welcome everyone to this morning's hearing on "Facial Recognition Technology: Examining Its Use by Law Enforcement."

Before we begin, I would like to remind Members that we have established an email address and distribution list dedicated to circulating exhibits, motions, or other written materials that Members might want to offer as part of our hearing today. If you would like to submit materials, please send them to the email address that has been previously distributed to your offices and we will circulate the materials to Members and staff as quickly as we can.

I would also ask all Members to mute your microphones when you are not speaking. This will help prevent feedback and other technical issues. You may unmute yourself any time you seek recognition.

I will now recognize myself for an opening statement.

As I said, good morning and welcome to a very important hearing, one that I hope will generate not only an understanding, but as I will ask a number of Witnesses, legislative fixes that may be relevant and important in this rise of technology matched against a document that has been a living document for more than a century, obviously, centuries, and that is the Constitution of the United States of America.

Like many other leaps forward in technology, facial recognition technology offers our society both promise and peril. Proponents extol the potential benefits of modernized policing, greater certainty in law enforcement, safer borders, and ultimately a more efficient criminal justice system.

At the same time, facial recognition systems have clear potential for misuse and have been found to be inaccurate at identifying certain groups of people.

Moreover, the technology and how it has been used in prosecution raises, as I said earlier, constitutional concerns that call into question the basic tenets of fairness and due process underpinning all criminal prosecution.

The criminal consequences implicated by these darker elements of facial recognition technology warrant closer examination by this body. Congress has found itself at a disadvantage in understanding this powerful tool because the information on how law enforcement agencies have adopted facial recognition technology remains under-reported or nonexistent.

Today, we are bringing facial recognition technology out of the shadows and into the light. This dialogue must start with the simple question of whether this technology is sufficiently accurate to justify its use by the police and if the risks of depriving someone of their liberty unjustly are too great.

To add untested and unvetted facial recognition technology to our policing would only serve to exacerbate the systemic issues still plaguing our criminal justice system.

Worse, large-scale adoption of this technology would inject further inequity into a system at a time when we should be moving to make the criminal justice system more equitable for Americans, as we're working very hard to pass the George Floyd Justice in Policing Act that was passed out of this particular Committee some many, many months ago.

There are many unknowns, but we can be certain of one thing: Most, if not all, facial recognition systems are less accurate for people of color and women. For the most part, we can be confident that the darker your skin tone, the higher the error rate.

Studies have found error rates in facial recognition software to be up to 34 percent higher for darker-skinned women than lighter-skinned men. It is not just sometimes wrong, it can be wrong up to a third of the time.

Additionally, a 2019 study by the National Institute of Standards and Technology found empirical evidence that most facial recognition algorithms exhibit demographic differentials that can worsen their accuracy based on a person's age, gender, or race. According to the study, systems varied widely in their accuracy and depending on the algorithm and type of search.

America is a multicultural, multi-ethnic Nation. This is particularly important as relates to these findings.

Asian and African-American people were up to 100 times more likely to be misidentified than White men. Native Americans had the highest false positive rate of all ethnicities.

Women were more likely to be falsely identified than men. The elderly and children were more likely to be misidentified than those in other age groups. It could play a really strong role in trying to find missing persons, for example, if it was to be used in that.

Middle-aged White men generally benefited from the highest accuracy rate.

Yet, in spite of these flaws, facial recognition technology is being rolled out across the country and has in many instances proven valuable to law enforcement. From the largest Federal law enforcement agencies to small local police departments, facial recognition systems are quietly be incorporated into American policing.

There lies the complexity, because you have small departments, 18,000 in the United States, that may not have the training and are using these technologies.

We have heard the success stories, such as facial recognition technology being used to identify the shooter in the tragic Capital Gazette massacre and to help identify victims of sex trafficking by matching missing persons photos to online ads.

Most recently we have learned that facial recognition technology has been used to identify several of the insurrectionists who stormed the citadel of American democracy on January 6.

However, while we must applaud the utilization of new technology for the apprehension of domestic terrorists, this must be weighed against the fact that many of the systems, both privately owned or owned by government entities, operate with minimal transparency, limited oversight, and questionable informational security.

Let me remind you again, 18,000 different police departments across America of varying sizes, varying training, and varying technology capability. Again, it is noted that they are using technology, again, with minimal transparency, limited oversight, and questionable informational security.

In some cases, individual employees are testing this private software without the knowledge or approval of their superiors or supervising agencies.

Without notice, many communities find facial recognition systems deployed in their neighborhoods. The adoption and use of facial recognition systems must involve community consideration, technological evaluation, and sober legal analysis.

As these trends have developed, the Federal Government has been largely absent. What we do not know towers over what we do, and that needs to change. Seemingly little thought has been put into the widespread adoption of a technology that could materially alter community interactions with law enforcement.

This is the issue this Committee hopes to correct today and going forward. This hearing is not meant to prejudge facial recognition technology or its value to law enforcement, but rather it is an im-

portant first step to proactively engage with this technology and adapt our laws accordingly.

As I indicated, it is important that out of this Committee hearing we also work on productive and constructive legislation as needed.

I am looking forward to engaging with the Witnesses about the benefits and pitfalls inherent in facial recognition technology and to forging a way forward towards transparency, equity, and accountability in its use.

It is now my pleasure to recognize the Ranking Member of the Subcommittee, the gentleman from Arizona, Mr. Biggs, for his opening statement.

Mr. BIGGS. Madam Chair, thank you for yielding time to me and I thank you for holding this very important hearing on facial recognition technology and its use by law enforcement.

I think there is so much of what you just said that I can associate myself with. There are some things that we can work together on a bipartisan basis, not just you and I, but hopefully all the Members of the United States Congress.

Facial recognition technology is a powerful tool when used properly. When used improperly or relied upon too heavily, it raises some very serious concerns and has some very real world negative consequences.

Today, we'll hear from a Witness who was detained after the Detroit Police Department relied on facial recognition technology that pointed a finger wrongly at this man.

Facial recognition technology is not perfect—and actually, quite honestly, it's far from it. To be reliable, images must be captured in the most favorable conditions with lighting, angle, aging, and other factors ultimately reducing reliability.

Worse yet, facial recognition algorithms perform poorly when tasked with analyzing the faces of women, people of color, elderly, and children.

I am also concerned about the potential First and Fourth Amendment erosions that facial recognition technology can cause. Law enforcement agencies could potentially use the systems for the surveillance of individuals not involved in any suspicious activity whatsoever.

Moreover, Federal law enforcement agencies with assistance from their State and local law enforcement partners have access to images of an overwhelming number of otherwise law-abiding citizens. State and motor vehicle agencies possess high-quality photographs of most citizens that are a natural source for facial recognition programs and could easily be combined with public surveillance or other cameras in the construction of a comprehensive system of identification and tracking.

Federal law enforcement agencies are also not limited to facial recognition technology systems they control or those controlled by other law enforcement partners at the State and local level. Federal law enforcement can use nongovernment facial recognition service providers, such as Vigilant Solutions or Clearview AI.

For example, law enforcement officers with a Clearview AI account can use a computer or smartphone to upload a photo of an unknown individual with Clearview AI's facial recognition system. The system then returns search results that show potential photos

of the unknown individual as well as links to sites where the photos were obtained, such as Facebook or Instagram.

The use of facial recognition technology is largely unregulated and raises numerous concerns. The government could use facial recognition technology to monitor or target people exercising their First Amendment rights, including freedom of association.

Facial recognition technology also poses significant privacy concerns, and improper use could violate the Fourth and First Amendment rights protecting people from unreasonable searches and seizures and guaranteeing freedom of association.

With these constitutional reliability concerns with this technology, the GAO just issued a report indicating that not only had the Federal law enforcement agencies not assessed privacy and other risks associated with the use of this technology, but some of them don't also even know which systems their agents are using.

So, in sum, I think this is a real opportunity for us to gain some important information and knowledge today. I have enormous concerns that I will summarize here.

The technology here is absolutely problematic and inconsistent. It's not been perfected. Images of law-abiding people have been acquired. The security of the databases is an issue, as we have seen with recent breaches of databases. Private companies acquiring and scraping information and data and selling it to the feds and other law enforcement. Manipulation and enhancements of photos can take place. It expands the surveillance State that we have been railing against. The GAO report gave some important concerns.

Those are just some of my—that's a brief summary of some of these things that I am concerned with. I do think it's a place where we can work, Madam Chair, to find common ground.

If we're talking about nationalizing police forces, I don't think we'll get there. If we're talking about finding some kind of meaningful regulation and oversight of the implementation of facial recognition technology, which I think is what the Chair is alluding to, then I think we can find a lot of common ground here.

With that, Madam Chair, I would like to submit for the record a letter to the Committee dated July 12, 2021, from Matthew Feeney of the Cato Institute.

Ms. JACKSON LEE. You want to finish the letter explanation?

Mr. BIGGS. Yes. Yes, if I can, please.

Also, I wish to submit an article from American Military News from July of 2021 regarding the Capitol Police adoption of Army surveillance gear to monitor Americans and identify threats.

I also wish to include several articles about the Alaskan couple that through facial recognition technology that was erroneously used. One would be an AP news article on riots, technology, capitol siege, and government and politics, another one from Alaska's News Source, and another one from *Homenews.com*, if it's possible, Madam Chair.

Ms. JACKSON LEE. Without objection, so ordered.

[The information follows:]

MR. BIGGS FOR THE RECORD



July 12, 2021

The Honorable Sheila Jackson Lee
Chair
Subcommittee on Crime, Terrorism,
& Homeland Security
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Andy Biggs
Ranking Member
Subcommittee on Crime, Terrorism,
& Homeland Security
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Chairwoman Lee, Ranking Member Biggs, and Members of the Subcommittee:

My name is Matthew Feeney. I am the director of the Cato Institute's Project on Emerging Technologies. My research is focused primarily on how new and emerging technologies affect civil liberties. Facial recognition is one of the most concerning of these technologies, so I appreciate the opportunity to provide input in connection with this panel's July 13 hearing, titled "Facial Recognition Technology: Examining Its Use by Law Enforcement."

I believe that it is possible to craft regulations and legislation that would address the most worrying uses of facial recognition technology without hampering innovation. Below, I will highlight why I think such regulation and legislation are necessary before providing an overview of specific policy recommendations.

Risks and Benefits of Facial Recognition

Facial recognition technology confirms an individual's identity via automated analysis of images. Most means of identity verification, such as driver's licenses and passports, are easily concealed, and there is a body of law that governs how a law enforcement officer can legally request such documents. Yet our faces are not so easy to conceal, and facial recognition requires only a camera linked to the necessary software to work.

Although facial recognition has been available for decades in one form or another, recent improvements in the technology and the plethora of private and public images related to law abiding citizens means that left unchecked it poses an unprecedented risk to Americans' privacy.

Sadly, foreign countries have shown us what a society with widespread use of government facial recognition looks like. Chinese law enforcement officials use facial, behavioral, and ethnic recognition technologies to supplement an already extensive and oppressive surveillance state.¹ Perhaps the most horrifying of this

¹ Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *The New York Times*, July 8, 2018. <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html>

surveillance is taking place in China's Xinjiang province, where the Chinese Communist Party is implementing a policy of cultural cleansing of the predominantly Muslim Uyghur population.²

In the United States we are fortunate to enjoy far more civil liberty protections than the Chinese. But the history of American surveillance reveals that the United States is not immune to mass surveillance and that a long and diverse list of communities have found themselves on the receiving end of such snooping.³ Absent appropriate restrictions, facial recognition could be used in America's next episode of mass surveillance.

Like many other surveillance tools, facial recognition has valuable private sector applications. Facial recognition could one day make tickets lines at train stations, concerts, and cinemas a feature of the past. It could also be widely used for payments and to assist the visually impaired.⁴ It would be regrettable if the legitimate civil liberty concerns associated with facial recognition hampered these welcome innovations.

Federal Facial Recognition

Twenty federal agencies, which combined employ around 120,000 law enforcement officers, reported using facial recognition technology systems during a recent survey conducted by the Government Accountability Office (GAO).⁵ These systems can access billions of images.⁶ Ten of the surveyed agencies (including the Federal Bureau of Investigation, the Drug Enforcement Administration, and the U.S. Customs and Border Protection) use Clearview AI, a facial recognition search engine that allows users to search billions of images uploaded to popular social media platforms. According to reporting from BuzzFeed, the GAO report may have

Seungha Lee, "Coming into Focus: China's Facial Recognition Regulations," Center for Strategic & International Studies, May 4, 2020. <https://www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations>

² Jane Wakefield, "AI emotion-detection software tested on Uyghurs," BBC News, May 26, 2021. <https://www.bbc.co.uk/news/technology-57101248>

Human Rights Watch, "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," May 1, 2019. <https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass>

³ American Big Brother," Cato Institute, accessed July 8, 2021, <https://www.cato.org/american-big-brother>.

⁴ Richard Baimbridge, "Why your face could be set to replace your bank card," BBC News, January 24, 2021. <https://www.bbc.co.uk/news/business-55748964>

Lindsay Reynolds, Shaomei Wu, "Designing a face recognition application for people with visual impairments," Facebook Research, April 23, 2018. <https://research.fb.com/blog/2018/04/designing-a-face-recognition-application-for-people-with-visual-impairments/>

⁵ U.S. Government Accountability Office, Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks, GAO-21-518 (Washington, DC, 2021), 8, accessed July 11, 2021, <https://www.gao.gov/assets/gao-21-518.pdf>

⁶ Ibid.

undercounted the number of federal law enforcement agencies that have used Clearview AI's technology.⁷

The vast majority of the billions of images available to federal law enforcement officers using facial recognition systems are associated with law abiding citizens and residents. Many of these images are scraped from non-government entities, but some come from public agencies such as state departments of motor vehicles, creating what Georgetown researchers have described as the "perpetual lineup."⁸

It is this "perpetual lineup" that ought to most concern lawmakers. Below are policies that would protect civil liberties while allowing law enforcement officials to use facial recognition technology.⁹

- 1) Database restrictions: Law enforcement facial recognition databases should only include data related to those with outstanding warrants for violent or other serious crimes. These databases should undergo regular purges of irrelevant data.

Law enforcement should only be able to add data related to someone to the database if they have probable cause that person has committed a violent or other serious crime. Relatives or guardians of missing persons (kidnapped children, those with dementia, potential victims of accidents or terrorist attacks) should be able to contribute relevant data to these databases and request their prompt removal.

Such a policy need not restrict law enforcement from using facial recognition systems trained with data related to those without outstanding warrants. The policy merely restricts the library of images law enforcement can search.

- 2) Open source/data requirement: The source code for the facial recognition system as well as the datasets used to build the system should be available to anyone. This will help improve accountability and transparency and is of particular urgency given concerns associated with facial recognition technology and racial bias.¹⁰

⁷ Caroline Haskins, Ryan Mac, "A Government Watchdog May Have Missed Clearview AI Use By Five Federal Agencies In A New Report," BuzzFeed, June 30, 2021.

<https://www.buzzfeednews.com/article/carolinehaskins1/gao-facial-recognition-report-clearview-federal-agencies>

⁸ Clare Garvie, Alvaro Bedoya, Jonathan Frankle, "The Perpetual Lineup: Unregulated Police Face Recognition in American," Georgetown Law, October 18, 2016.

<http://www.perpetuallineup.org>

⁹ These policies recommendations are adapted from policies discussed here:

Matthew Feeney, "Should Police Facial Recognition Be Banned?" Cato Institute At Liberty blog, May 13, 2019. <https://www.cato.org/blog/should-police-facial-recognition-be-banned>

¹⁰ Alex Najibi, "Racial Discrimination in Face Recognition Technology," Harvard University Science in the News (SITN) blog, October 24, 2020.

- 3) Public hearing requirement: Law enforcement agencies should not be permitted to use facial recognition technology without first having informed the public about the planned use, released details about how the technology works, and allowed ample time (e.g. six months) for public comment.
- 4) Threshold requirement: Use of facial recognition should be delayed until law enforcement can demonstrate at least a 95 percent identity confidence threshold across a wide range of demographic groups (gender, race, age, etc.).¹¹

Such policies would significantly restrict the number of images law enforcement collect for facial recognition searches, increase transparency and accountability, and protect those engaged in First Amendment-protected activities such as protests and religious gatherings. They would also allow private companies to develop facial recognition systems without having to worry that their images of customers will be included in law enforcement facial recognition searches.

Thank you for your attention to this important issue. I welcome the opportunity to discuss facial recognition further.

Sincerely,



Matthew Feeney
Director, Project on Emerging Technologies
Cato Institute

<https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/>

¹¹ The identity confidence threshold need not be 95%, but arguments in favor of a lower threshold should be met with scrutiny. Amazon recommends a 95% confidence threshold for law enforcement use of its facial recognition system.

William Crumpler, "How Accurate are Facial Recognition Systems – and Why Does It Matter?" Center for Strategic & International Studies, April 14, 2020.

<https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems---and-why-does-it-matter>

8/17/22, 11:34 AM

Capitol Police to use Army surveillance gear to monitor Americans and 'identify emerging threats' | American Military News

Capitol Police to use Army surveillance gear to monitor Americans and 'identify emerging threats'

A americanmilitarynews.com/2021/07/capitol-police-to-use-army-surveillance-gear-to-monitor-americans-and-identify-emerging-threats

Liz George

July 12, 2021



U.S. Capitol Police will start using Army surveillance equipment to monitor Americans as part of a larger effort to improve security and turn the force into “an intelligence-based protective agency” in the wake of the storming of the U.S. Capitol on January 6.

Last week, the USCP took possession of eight Persistent Surveillance Systems Ground – Medium (PSSG-M) units, fulfilling a request that Defense Secretary Lloyd Austin approved on June 2. The units capture high-definition video and include night vision, but do not feature facial recognition capabilities.

“This technology will be integrated with existing USCP camera infrastructure, providing greater high definition surveillance capacity to meet steady-state mission requirements and help identify emerging threats,” the Pentagon said.

The same technology was used by troops during the wars in Iraq and Afghanistan to observe large areas day and night.

The Army will install the units and train Capitol Police on how to operate the systems, the Pentagon said.

In a statement last week, the USCP called the technology “state-of-the-art campus surveillance technology, which will enhance the ability to detect and monitor threat activity.”

The Capitol Police did not provide further details regarding how or where the surveillance equipment would be used, and didn't provide information on whether data collected would be stored or distributed.

These latest efforts by the Capitol Police have raised some concerns relating to Americans' privacy rights. Last month, a federal appeals court found similar surveillance technology used by the Baltimore Police Department (BPD) violated the constitution's Fourth Amendment protections against unreasonable search and seizure.

A New York University School of Law independent audit of the systems used by the BPD found the technology allowed the department to track individuals for multiple days.

William Owen, a member of the Surveillance Technology Oversight Project, said the Capitol Police's new technology is cause for concern.

“These so-called improvements that the Capitol Police have implemented after the insurrection represent an expansion of police power and surveillance that STOP cautioned against in January,” he said, according to The Washington Times.

“As awful as the events on Jan. 6 were, increased use of biased surveillance technology is never the answer,” he said. “Such technology will inevitably be used to target Black, brown, and Muslim communities and protesters, not White, racist, far-right mobs like those who were given free rein to enter the Capitol. So we need greater civilian oversight of police, not greater police power.”

The report comes after the USCP announced it will open regional offices nationwide, beginning in California and Florida, in order to “investigate threats” made against members of Congress.

A report from Roll Call last summer noted that the USCP is currently exempt from the Freedom of Information Act (FOIA) because it is part of the legislative branch, giving it a level of secrecy and a lack of established accountability methods that aren't the case for other law enforcement agencies.

“Congress is not subject to the law, and the Capitol Police, as a component of the legislative branch, is also exempt from any FOIA request,” the report stated.

8/17/22, 11:36 AM

Did agents raid home of wrong woman over Jan. 6 riot? Maybe. | AP News

Did agents raid home of wrong woman over Jan. 6 riot? Maybe.

[AP apnews.com/article/riots-technology-capitol-siege-government-and-politics-48477cd7e012926b04a74bbe68e477ef](https://apnews.com/article/riots-technology-capitol-siege-government-and-politics-48477cd7e012926b04a74bbe68e477ef)

May 5, 2021

By MARK THIESSEN and MICHAEL BALSAMO



1 of 3

FILE - In this Jan 6, 2021, file photo, U.S. Capitol Police try to hold back rioters outside the east doors to the House side of the U.S. Capitol. The volume of people inside the Capitol building, along with the lack of arrests made at the time of the riot, has made it difficult to identify people, even with the glut of social media evidence. Federal agents have dug through thousands of social media posts, used sweeping warrants to obtain information on cellphones in the area of the Capitol, facial recognition tools and logs of devices that logged into the congressional WiFi during the riot to try to identify the hundreds of people who stormed the Capitol. (AP Photo/Andrew Harnik, File)

ANCHORAGE, Alaska (AP) — “We’re looking for Nancy Pelosi’s laptop,” FBI agents told Marilyn Hueper after briefly handcuffing her.

<https://apnews.com/article/riots-technology-capitol-siege-government-and-politics-48477cd7e012926b04a74bbe68e477ef>

1/4

Hueper shot back: “That still doesn’t explain why you’re in my home. Or in Homer, Alaska.”

The search for the House speaker’s laptop had taken a U.S. Capitol Police officer thousands of miles away from home for an FBI raid on Hueper’s home, looking for something stolen during the Jan. 6 insurrection — and the person who did it.

The agents would walk out of Hueper’s home with iPads, cellphones and a pocket-sized copy of the Declaration of Independence. They took a laptop, but it wasn’t from Pelosi’s office. And it’s possible they may have the wrong person altogether — even though Hueper looks strikingly similar to the thief.

The Justice Department’s massive prosecution of those who stormed the U.S. Capitol on Jan. 6 has not been without its problems, including this potential instance of mistaken identity. And as Republicans are increasingly seeking to minimize the insurrection and play down the horror of the day, any missteps by federal prosecutors could be used in that effort to discredit what actually happened.

Federal prosecutors have charged more than 400 people, the largest undertaking by the department, including scores of defendants who posted images of their crimes online and boasted about breaking into the hallowed building. Some are facing serious charges and considerable prison time.

Hueper and her husband first came to officials’ attention this year when Alaska Airlines in February banned the couple for refusing to wear masks on a flight, according to court documents obtained by The Associated Press. Then two other people called in tips saying they recognized Hueper in photos that authorities had released of suspects wanted for storming the Capitol.

The insurrectionists sought to disrupt the certification of President Joe Biden’s victory. Hundreds of officers were injured and five people died after the riot, including a Capitol Police officer.

Supporters of then-President Donald Trump ransacked offices, rifled through lawmakers’ papers and desks, smashed through glass, shattered windows and tore down signs. Among the items stolen: the laptop from Pelosi’s office, her lectern, an iPad belonging to Majority Whip Rep. Jim Clyburn and other electronics.

But the volume of people inside the Capitol building, along with the lack of arrests made at the time of the riot, has made it difficult to identify people, even with the glut of social media evidence. Federal agents have dug through thousands of social media posts, gotten sweeping warrants to obtain information on cellphones in the area of the Capitol, used facial recognition tools and obtained logs of devices that signed into the congressional Wi-Fi during the riot.

But by far the most effective tool for federal agents has been old-fashioned tips. Many of the rioters have been ratted out by their friends and family members.

The warrant, obtained by the AP, identifies Hueper as the woman who took the laptop.

But they're wrong, Hueper insists. She told the AP that another woman wearing her same coat and with a similar hairstyle was inside the Capitol during the insurrection, not her. She admits she was in Washington, D.C., for Trump's rally that day but says she didn't get any closer than 100 yards (91 meters) from the Capitol and spent part of the day being lost in an unfamiliar city.

She said agents showed her one photo of the woman inside the Capitol, and they looked so similar that Hueper wondered if someone had used photo-editing software to put her in the photograph.

The warrant details how FBI agents located an image showing Hueper wearing similar clothing in a photo on her husband's Instagram account. It said Hueper's husband had also posted photos of them near the Capitol. "BEST OF 2020," he wrote in one, showing her from behind nearing the building. "Marilyn approaching the Capital. As Patriots, there is a righteous revolution to take back our country ... To be there was a once-in-a-lifetime experience. STOP THE STEAL!"

Hueper said an agent came back with a different and larger photo of the woman, which showed the suspected thief wearing a black sweater with large white snowflakes on it. The agent asked where in the house they could locate the sweater.

Hueper said she reiterated she wasn't inside the building. "No. 2, why didn't you show me this photo to start with? Because we can both obviously see here this is a different person."

Plus, she said, the sweater was hideous.

Hueper said she grabbed the photo and held it next to her face, asking the female agent to look at both closely, "Me. Her. Me. Her," she told the agent. Hueper said the agent grabbed the paper and walked off.

Both women were wearing black Columbia down coats. However, in a photo posted on her husband's Facebook page from Jan. 6, Hueper is shown wearing a black face mask, a green blouse open at the collar and a light green scarf. The surveillance video released by the FBI shows the sought-after woman wearing the black sweater with a snowflake print and dangling earrings. Also, the woman in the photo has detached earlobes, while Hueper says hers are attached.

After insisting, Hueper was shown the front page of the warrant but not allowed to thoroughly read the document, she said. She read it only after receiving a copy as the dozen or so agents and Capitol Police officer left.

According to the search warrants, agents could collect any electronics that might be suspected to have been involved, items stolen from the Capitol, a laptop with descriptors and a serial number — “which they didn’t find,” she said — and any paperwork related to planning violence.

Hueper said she has not heard back from federal authorities, nor have agents returned her laptop, two iPads, two cellphones or the 50-cent pocket-sized Declaration of Independence booklet they confiscated April 28.

She has not been arrested. Justice Department officials would say only that the investigation is ongoing.

But she decided to go public with her story, just in case.

“I better go online and protect myself before they call me in and make me this person,” she said.

Balsamo reported from Washington.

All contents © copyright 2022 The Associated Press. All rights reserved.

8/17/22, 11:38 AM

Search warrant reveals why the FBI raided an Alaska couple's home

Search warrant reveals why the FBI raided an Alaska couple's home

 [alaskanewssource.com/2021/05/05/search-warrant-reveals-why-the-fbi-raided-an-alaska-couples-home](https://www.alaskanewssource.com/2021/05/05/search-warrant-reveals-why-the-fbi-raided-an-alaska-couples-home)

By Jill Burke

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

IN THE MATTER OF THE SEARCH OF

 Homer, Alaska

Case No. 3:21-mj-00237-MMS

Filed Under Seal



Apr 22 2021

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Wendy Terry, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal

ANCHORAGE, Alaska (KTUU) - Newly unsealed court records show why Joint Terrorism Task Force investigators and a judge believed there was probable cause to search the premises of Paul and Marilyn Hueper in Homer in late April. The couple, who own the Homer Inn and Spa, attended the Jan. 6 rally at the nation's Capitol.

The Huepers have said they did nothing wrong.

In an interview last week, the Huepers told Alaska's News Source the FBI mistook Marilyn Hueper for a woman who'd entered the Capitol that day, and that during the search, agents said they were looking for Nancy Pelosi's laptop.

An affidavit filed in support of the search warrant states that on February 24, the FBI received a tip about the Huepers. The witness, who is not identified, told the FBI that Marilyn Hueper looked like a woman in tip line photos 225 A and 225 B the FBI had posted on its website. The FBI posted the photos in hopes the public could help locate individuals sought in connection with the Jan. 6 riots.

The witness, named only as “witness 1” in the affidavit, provided a copy of an Instagram post made by Paul Hueper, which appears to show Marilyn approaching the capitol steps wearing the same coat and purse as the woman sought by the FBI. That sought-after woman is seen in various images and video inside the capitol, including images showing her disconnecting the cords from Nancy Pelosi’s laptop and giving her gloves to an unidentified man to then remove the laptop.

The search warrant cites several federal crimes it believed may have been committed, including trespassing on Capitol grounds in restricted areas.

In applying for a search warrant, the FBI said it had “confirmed the woman in photograph’s (sic) 225 A and B was MARILYN HUEPER by comparing MARILYN HUEPER’s Driver License photograph.”

The FBI also said a second witness who knows Marilyn Hueper came forward on March 23 and confirmed Hueper as the woman in the photographs.

The Huepers say it’s a case of mistaken identity.

“You can visibly see with the photo that I’m the wrong person,” Marilyn Hueper said in a phone interview last week.

She said the agents seized computers, phones and a copy of the Declaration of Independence.

Marilyn Hueper said when she asked the FBI if they would admit she’s not who they are seeking, they told her “We’ll see if the information on your electronics supports what you’re saying. If it does, you don’t have anything to worry about.”

The search warrant allowed the FBI to search for electronics, clothing worn by the woman seen in the images they’d gathered from Jan. 6, Nancy Pelosi’s laptop and any other property stolen from the Capitol.

In an interview April 30, the Huepers told Alaska’s News Source they never entered the Capitol building and did not remove any items from the Capitol.

With the search over and the search warrant now public, the FBI declined to comment Wednesday on whether the agency stood by its identification of Marilyn Hueper as the same woman in the images on their website. Those images remain published on the FBI’s most wanted pages under the section on capitol violence.

In applying for the search warrant, the FBI successfully convinced the judge to seal — or keep secret — the warrant at the time “because the items and information to be seized are relevant to an ongoing undercover investigation and not all targets of the investigation will be searched at this time,” according to the court filing.

Copyright 2021 KTUU. All rights reserved.

Editor's note: This article has been updated with additional information.

Homer, Alaska

HOMER NEWS



NEWS

Homer residents said home was searched by FBI in connection to the Jan. 6 Capitol riots

Couple said agents seized computers, cell phones

By [Sarah Knapp](#) • April 29, 2021 1:30 am

Tags: [Crime](#), [Local News](#)



An official website of the United States government. Here's how you know.

[MORE](#) [HOME](#) [MOST WANTED](#) [CAPITOL VIOLENCE IMAGES](#)

FBI

MOST WANTED

[Ten Most Wanted Fugitives](#) [Fugitives](#) [Capitol Violence](#) [Terrorism](#) [Kidnappings/Missing Persons](#) [Parental Kidnapping](#)

Photograph #225 A

The FBI is seeking to identify individuals involved in the riots at the U.S. Capitol on January 6, 2021. Call 1-800-CALL-FBI or visit tips. Reference the photo number when calling or submitting information online. More at [fbi.gov/capitolviolence](#)



Size: 109KB

A screenshot from the FBI's Most Wanted page showing a photo the FBI said was taken on Jan. 6, 2021, inside the U.S. Capitol. Marilyn Hueper said FBI agents showed her this image and claimed it was her. (Screenshot)

Correction: The story has been updated to show the correct location of the Hueper home. It is on Ocean Drive Loop.

The FBI visited a Homer couple on Wednesday morning in what Marilyn and Paul Hueper claim is a case of mistaken identity related to the Huepers' participation in protests at the U.S. Capitol on Jan. 6.

According to a Facebook post by Marilyn Hueper on her husband Paul's Facebook page, FBI agents searched their Ocean Drive Loop home on April 28. The home also is the location of Homer Inn & Spa. Hueper shared on Facebook that they were startled when a dozen armed agents entered their home, quickly handcuffed them and their house guests, and began searching their home and interrogating them in regard to their activities Jan. 6 at the Capitol.

Quality local journalism is more important than ever.

SUPPORT OUR WORK

Official FBI details regarding the search are not available for public access at this time, but FBI Public Affairs Officer Chloe

Martin on Thursday confirmed that “the FBI was conducting court-authorized law enforcement activity at the location.” Martin said she could not comment further and that she could neither confirm nor deny that there is an investigation. The Huepers did not respond to emails, phone messages or texts by the Homer News seeking comment.

According to the Facebook post, Marilyn Hueper wrote that she was misidentified through photo recognition as a rioter who stormed the Capitol building. In an interview with “On Top of the World” talk show radio host Chris Story on Thursday, the couple said they did attend a protest on Jan. 6 in support of former President Donald Trump’s claim that the election was fraudulent. They said they got near the Capitol about 90 minutes after protesters first approached the Capitol and some entered the building. Marilyn Hueper told Story that agents showed her a photo of a woman with similar features to her who was inside the Capitol. She said the agents claimed the photo was of her. However, Marilyn Hueper said the woman in the photograph had different facial features, such as arched eyebrows and attached earlobes.

Marilyn Hueper said she later looked up the photo and that it is photograph #225a on the [FBI’s U.S. Capitol Violence Most Wanted website](#).

According to the interview with the Huepers on Story’s show, they said the FBI had a court-ordered search warrant for Speaker of the House Nancy Pelosi’s laptop and any other related items stolen from the Capitol during the riots, but did not present the warrant until hours after the search began. FBI agents confiscated their personal laptops and cell phones in search of evidence.

“This simply feels like a violation of those of us that were there that had every right, as President Trump said, to protest peacefully, so that’s what we did,” Paul Hueper said during the interview. “We were not inside the Capitol building. We didn’t condone any of the violence that took place there whatsoever.”

This is an ongoing story and will be updated as more information becomes available.

Reach Sarah Knapp at sarah.knapp@homernews.com.



A screenshot from the FBI's Twitter page showing a photo the FBI said was taken on Jan. 6, 2021, inside the U.S. Capitol. Marilyn Hueper said FBI agents showed her some of these images and claimed it was her. (Screenshot)

Tags: [Crime](#), [Local News](#)

[< Previous](#) | [Next >](#)
[Town Crier](#) | [Quick Flow Male Enhancement Pills \[Review\] Legit or Cheap?](#)

Stevens, Vance lead in unofficial primary results

Floralite Reviews: Is It Legit? What They Won't Ever Tell You!

CircadiYin Review: What They Won't Ever Tell You

The Lost Superfoods Book Review: Is It Legit?

Dr Marty's Nature's Blend Dog Food Reviews – Is It Legit?

Sign Up For Our Newsletters

Subscribe to our e-mail newsletter to receive updates.

 SIGN UP

Ms. JACKSON LEE. I thank the Ranking Member of the Subcommittee for his presentation and his opening statement.

I do believe that, as I indicated, we should be engaged in both oversight and legislative response, and I would like to find common ground with our colleagues. Because I think this is very, very important both in terms of law enforcement and the utilization thereof, but also for the constitutional principles which we all believe in.

It's now my pleasure to recognize the distinguished Chair of the Full Committee, the gentleman from New York, Chair Nadler, for his opening statement.

Chair NADLER. Well, thank you very much. I thank Chair Jackson Lee for convening this hearing on the use of facial recognition by law enforcement.

Facial recognition technology is now able to capture images and analyze them in ways that would have been completely impossible only a decade ago. In some cases, the technology enables the real-time surveillance and matching of individuals in a crowd.

As facial recognition technology has proliferated in a manner largely unchecked by Congress, we now live in a world where biometric data is collected by private businesses, schools, State and local agencies, and as is the focus of this hearing, by law enforcement agencies at all levels of government.

There is a tension that we must address. On the one hand, this technology is now a commonplace fixture in our lives. On the other hand, most Americans have little understanding of how the police use facial recognition technology to conduct surveillance of communities across the country—for better for or worse.

Thanks to the work of the Government Accountability Office, we have our first glimpse into Federal law enforcement's use of facial recognition technology. In its recent study, GAO found that 20 of the 42 Federal law enforcement agencies surveyed used some form of facial recognition technology.

This report, although an important first step, leaves many unanswered questions about how the technology is used, when it is used, and what type of mechanisms are in place to guard against abuse or to protect sensitive data.

For example, of the 14 Federal agencies that said they used non-Federal systems, only one agency could provide the GAO with complete information about what systems their employees were actually using in the field.

The picture at the State and local level is even more opaque, but we have received several disturbing reports of the misapplication of facial recognition technology by local police departments. For example, this technology has proven particularly unreliable when attempting to match women and people of color.

In some cases, facial recognition is deployed without proper consideration of due process rights. One Witness here today, Mr. Williams, will testify to the profound impact that misidentification under these circumstances can have on an individual's life.

Simply put, Mr. Williams deserves better from the law enforcement agencies entrusted to use a technology that we all know is less accurate when applied to citizens who look like him.

Facial recognition technology can be an important crime-fighting tool. Like all such tools, we need to ensure that the adoption of this

new technology does not further erode trust between law enforcement and the communities they serve and does not compound the unfairness of a criminal justice system that too often disproportionately impacts people of color.

Today, this Subcommittee begins to ask the critical questions surrounding police use of facial recognition technology. The hearing will not answer every question about the adoption of facial recognition technology by law enforcement, but my hope is that we will take another important step toward balancing the needs of law enforcement agencies, the priority of keeping Americans safe from crime, and the valid concerns about this technology expressed by communities across this country.

Our task is not an easy one. We want an America where every individual knows that they and their families are safe from harm, while our fundamental rights are protected. We want an America where law enforcement has the tools it needs to protect and serve, but with clear guidelines and rules that prevent those tools from being abused.

Understanding how to make that vision real at a moment when technology keeps changing and evolving will take a tremendous amount of work, but this is work worth doing.

Again, I thank the Chair for calling this hearing. I look forward to hearing from our Witnesses, especially Bertram Lee, who once worked for my office way back when.

It's good to see you, and I look forward to your testimony.

I thank all the Witnesses for taking their time to engage with us on this important topic, and I look forward to their testimony.

I yield back the balance of my time.

Ms. JACKSON LEE. I thank the Chair very much for his important presentation.

Now, it's my pleasure to recognize the distinguished Ranking Member of the Full Committee, the gentleman from Ohio, Mr. Jordan, for his opening statement.

Mr. JORDAN. Thank you, Madam Chair.

I look forward to today's hearing on facial recognition technology. I am hopeful we can approach this issue in a truly bipartisan manner, as has been mentioned by some previous statements.

Last Congress, we worked closely with our colleague, the late Chair Elijah Cummings, on this very issue. While we had many vigorous debates on a variety of issues, facial recognition technology was one issue where we shared common ground. So much so, that we held three bipartisan hearings in the Oversight Committee on this technology.

In those hearings, we learned many important facts about facial recognition technology. There are serious First and Fourth Amendment concerns about the use of FRT by law enforcement.

There are also due process concerns about how law enforcement uses this technology. We learned, for example, that over 20 States' departments of motor vehicles have handed over their driver's license data to the FBI.

No American citizen gave their consent to have their data and images turned over to the FBI. No elected official ever voted to allow this to happen. Every American should be troubled by this.

I know I am, and I hope my colleagues on this Committee are as well.

Almost two weeks ago, the GAO issued a new report about how Federal law enforcement uses FRT. This report makes clear that the Federal law enforcement agencies using facial recognition technology haven't even assessed the risk when using this technology. If they haven't even assessed the risks, they certainly aren't taking them into consideration when they're using the technology.

GAO has surveyed Federal law enforcement agencies on their use of facial recognition technology; 14 agencies that reported using the technology to support criminal investigations also reported using systems owned by non-Federal entities. Only one agency had awareness of what non-Federal systems are used by its employees.

In other words, not only are Federal law enforcement agencies not assessing the risk of using facial recognition technology, most don't even know which systems their employees are using.

I imagine it's difficult for a Federal agency to assess the risk of using a system if it doesn't even know which system it is using.

I look forward to learning more from GAO on this recent report and our other Witnesses on the path forward.

With that, Madam Chair, I yield back.

Ms. JACKSON LEE. I thank the gentleman for his opening statement.

Without objection, all other opening statements of our Members will be included in the record.

I will now introduce today's Witnesses, and let me again thank them for their participation. This is a virtual hearing that is no less crucial and important, and we thank you for participating in that manner of technology.

The first Witness is Director Gretta Goodwin. Gretta L. Goodwin is a Director in the Homeland Security and Justice team at the U.S. Government Accountability Office where she leads GAO's work on justice and law enforcement issues. Her portfolio includes Federal law enforcement oversight and training, civil liberties, civil rights, vulnerable populations, the Federal prison system, and the Federal judiciary.

Director Goodwin has a Ph.D. and a master's degree in economics from the University of Nebraska, Lincoln, and a bachelor's degree in economics from the University of Houston.

I am glad to see there's a Houston connection and the university that I happen to represent.

Welcome.

Professor Barry Friedman serves as a Faculty Director of the Policing Project at New York University School of Law where he is the Jacob D. Fuchsberg Professor of Law and affiliated professor of politics.

Professor Friedman has taught, litigated, and written about constitutional law for the Federal courts, policing, and criminal procedure for over 30 years, and has produced numerous books and articles, appearing in various scholarly journals and popular media outlets.

Professor Friedman graduated with honors from the University of Chicago and received his law degree magna cum laude from Georgetown University Law Center.

Welcome.

Robert Williams is a 43-year-old man who lives in Farmington Hills, Michigan, with his wife and two young daughters. He works as a logistics planner in the automotive industry. Mr. Williams was wrongfully arrested by the Detroit Police Department in 2020 when facial recognition technology misidentified him.

Mr. Williams, we apologize to you and very grateful for the testimony that you will be presenting here today.

Welcome.

Bertram Lee, Jr., is a counsel for media and technology at the Leadership Conference on Civil and Human Rights where he works to advance the interests of marginalized communities in technology and media policy. His portfolio includes broadband access, media diversity, facial recognition, law enforcement surveillance technology, section 230 of the Communications Decency Act, and algorithmic bias in artificial intelligence.

Previously, Mr. Lee worked as Policy Counsel at Public Knowledge and at the U.S. House Committee on Education and Labor under Chair Robert C. Scott.

He received his J.D. from Howard University School of Law and his B.A. from Haverford College.

Welcome.

Kara Frederick is a Research Fellow at the Center for Technology Policy at the Heritage Foundation. Her research focuses on Big Tech and emerging technology policy.

Among her prior roles, Ms. Frederick was a fellow at the Center for New American Security, served as a Senior Intelligence Analyst for a U.S. Naval Special Warfare Command, and helped create and lead Facebook's Global Security Counterterrorism Analysis Program.

She received her M.A. in war studies from King's College London and her B.A. in foreign affairs and history from the University of Virginia.

Welcome.

Professor Jennifer Laurin serves as the Wright C. Morrow Professor at the University of Texas School of Law where she studies and writes about how law and institutional design shape the functioning of criminal justice institutions.

She also currently serves as reporter to the American Bar Association's Criminal Justice Standards Task Force and is a former Chair of the Texas Capital Punishment Assessment team organized under the auspices of the American Bar Association.

Professor Laurin received her undergraduate degree in politics from Earlham College and her J.D. from Columbia Law School.

Welcome to you from Texas.

Brett Tolman is the Executive Director for Right on Crime. He is the founder of the Tolman Group and previously served as a shareholder at the law firm of Ray Quinney & Nebeker PC.

Previously, Mr. Tolman also served as the U.S. attorney for the District of Utah and was selected by Attorney General Michael Mukasey to serve as a special adviser to the Attorney General on national and international policy issues affecting United States attorneys in the Department of Justice.

Prior to becoming U.S. attorney, Tolman served as legal counsel to the United States Senate Judiciary Committee.

He received his B.A. and his J.D. from Brigham Young University.

Welcome.

Dr. Cedric Alexander is a law enforcement expert with over 40 years of experience in public safety. He has appeared on national media networks to provide comment on police-community relations and has written numerous editorials and books on the subject.

Previously, Dr. Alexander has served as Deputy Commissioner of the New York State Division of Criminal Justice Services, as Chief of Police of DeKalb County, Georgia, and as national President of the National Organization of Black Law Enforcement Executives, a very powerful law enforcement organization. He was also appointed to serve on President Obama's Task Force on 21st Century Policing.

He received a B.A. and a master's degree from St. Thomas University in Miami, Florida, and a doctorate from Wright State University.

Welcome.

Usually, I stand when I provide the oath, but we welcome our distinguished Witnesses and we thank them for their participation today. So, I will begin by swearing in our Witnesses.

If you would please turn on your audio. Make sure I can see your face and your raised right hand while I administer the oath. Please unmute and let me see your raised right hand.

Do you swear or affirm, under penalty of perjury, that your testimony you are about to give today to be true and correct to the best of your knowledge, information, and belief, so help you God?

I need to hear an audible "I do."

Thank you so very much.

Let the record show the Witnesses have answered in the affirmative.

Thank you so very much.

Please note that each of your written statements will be entered into the record in its entirety. Accordingly, I ask that you summarize your testimony in five minutes. There is a timer in the Zoom view that should be visible on your screen.

Director Goodwin, you may begin. Welcome. You are recognized for five minutes.

STATEMENT OF GRETTA L. GOODWIN

Dr. GOODWIN. Thank you Chair Nadler, Chair Jackson Lee, Ranking Member Jordan, Ranking Member Biggs, and Members of this Subcommittee, I am pleased to be here today to discuss Federal law enforcement's use of facial recognition technology.

Use of this technology has expanded in recent years, and questions exist regarding the accuracy of the technology, the transparency in its usage, and the protection of privacy and civil liberties when the technology is used.

Today, I will discuss:

- (1) The ownership and use of facial recognition technology by Federal agencies that employ law enforcement officers;
- (2) the types of activities these agencies use the technology to support; and

- (3) the extent that these agencies track employee use of the technology, especially those owned by non-Federal entities, as well as the potential privacy and accuracy implications.

We surveyed 42 Federal agencies that employ law enforcement officers. Twenty of them report that they owned a system with facial recognition technology or used another entity's system.

Of these 20 agencies, three own their own system, 12 only used another entity's system, and five agencies both owned a system and used another entity's. These agencies noted that some systems can include hundreds of millions or billions of photos.

Federal agencies reported using facial recognition technology to support various activities, such as criminal investigations, surveillance, and managing business operations during the COVID-19 pandemic.

Of the 20 agencies that owned or used the technology, 14 reported using it to support criminal investigations, including investigations of violent crimes, credit card and identity fraud, and missing persons.

Looking more closely at these 14 agencies, some of them told us that they used the technology last summer to support criminal investigations related to civil unrest, riots, or protests following the killing of Mr. George Floyd in May of 2020.

In addition, a few of these agencies told us they used the technology on images from the U.S. Capitol attack on January 6 of this year to generate leads for criminal investigations.

Of these 14 agencies, we found that 13 did not have complete, up-to-date information on what non-Federal systems are being used by their employees. So, agencies have not fully assessed the potential risk related to privacy and accuracy of using these systems.

To be clear, some agencies knew that employees were using certain systems. For example, agencies may have had formal agreements with States or contracts with private companies.

However, many agencies had to poll their employees to answer our questions. Multiple agencies initially told us they didn't use the technology and later changed their answers after talking with employees.

What these 13 agencies all have in common is that they don't have a process to track what Federal systems employees are using.

Although the accuracy of facial recognition technology has increased dramatically in recent years, risk still exists that searches will produce inaccurate results. If a system is not sufficiently accurate, it could unnecessarily identify innocent people as investigative leads.

The system could also miss investigative leads that would otherwise have been revealed.

Moreover, the technology's high error rates for certain demographic groups could result in adverse consequences for individuals.

Accordingly, we recommended that agencies implement a mechanism to track what non-Federal systems with facial recognition technology are used by employees to support investigative activities and assess the risk of using such systems, including privacy- and accuracy-related risks.

Facial recognition technology's capabilities are only going to grow stronger. If law enforcement agencies do not know if or how their employees are using the technology, then they cannot ensure that the appropriate protections are in place.

Chair Nadler, Chair Jackson Lee, Ranking Member Jordan, Ranking Member Biggs, and Members of this Subcommittee, this concludes my remarks. I am happy to answer any questions you have.

[The statement of Dr. Goodwin follows:]



United States Government Accountability Office

Testimony

Before the Subcommittee on Crime,
Terrorism, and Homeland Security,
Committee on the Judiciary, House of
Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Tuesday, July 13, 2021

FACIAL RECOGNITION TECHNOLOGY

Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees

Statement of Greta L. Goodwin, Director,
Homeland Security and Justice

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO@100 Highlights

Highlights of [GAO-21-105309](#), a testimony before the Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, House of Representatives

Why GAO Did This Study

Federal agencies that employ law enforcement officers use facial recognition technology to assist criminal investigations, among other activities. For example, the technology can help identify an unknown individual in a photo or video surveillance.

This statement describes (1) the ownership and use of facial recognition technology by federal agencies that employ law enforcement officers, (2) the types of activities these agencies use the technology to support, and (3) the extent that these agencies track employee use of facial recognition technology owned by non-federal entities, including the potential privacy and accuracy implications.

This statement is based on GAO's June 2021 report on federal law enforcement's use of facial recognition technology (GAO-21-518). To conduct that prior work, GAO administered a survey questionnaire to 42 federal agencies that employ law enforcement officers regarding their use of the technology. GAO also reviewed relevant documents and interviewed agency officials. The June 2021 report was a public version of a sensitive report that GAO issued in April 2021. Information that agencies deemed sensitive was omitted from the June 2021 report and this statement.

What GAO Recommends

In June 2021, GAO made two recommendations to each of 13 federal agencies to implement a mechanism to track what non-federal systems are used by employees, and assess the risks of using these systems. Agencies generally concurred with the recommendations.

View [GAO-21-105309](#). For more information, contact Gretta L. Goodwin at (202) 512-8777 or goodwin@gao.gov.

July 13, 2021

FACIAL RECOGNITION TECHNOLOGY

Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees

What GAO Found

In June 2021, GAO reported the results of its survey of 42 federal agencies that employ law enforcement officers about their use of facial recognition technology. Twenty reported owning systems with the technology or using systems owned by other entities, such as state, local, and non-government entities (see figure).

Ownership and Use of Facial Recognition Technology Reported by Federal Agencies that Employ Law Enforcement Officers



Source: GAO analysis of survey data. | GAO-21-105309

Note: For more details, see figure 1 in [GAO-21-105309](#).

Agencies reported using the technology to support several activities (e.g., criminal investigations) and in response to COVID-19 (e.g., verify an individual's identity remotely). Six agencies reported using the technology on images of the unrest, riots, or protests following the killing of Mr. George Floyd in May 2020. Three agencies reported using it on images of the U.S. Capitol attack on January 6, 2021. Agencies said the searches used images of suspected criminal activity.

Fourteen of the 42 agencies reported using the technology to support criminal investigations. However, only one had a mechanism to track what non-federal systems were used by employees. By having a mechanism to track use of these systems and assessing the related risks (e.g., privacy and accuracy-related risks), agencies can better mitigate risks to themselves and the public.

United States Government Accountability Office

Chair Jackson Lee, Ranking Member Biggs, and Members of the Subcommittee:

I am pleased to be here to discuss federal law enforcement's use of facial recognition technology. Use of this technology has expanded in recent years, raising concerns about privacy and the accuracy of facial recognition systems. Members of Congress and academics have highlighted the importance of understanding what technologies are owned and how they are used by federal law enforcement.

My statement today will focus on (1) the ownership and use of facial recognition technology by federal agencies that employ law enforcement officers, (2) the types of activities these agencies use the technology to support, and (3) the extent that these agencies track employee use of facial recognition technology owned by non-federal entities, including the potential privacy and accuracy implications. This statement is based on findings from our June 2021 report, which included the results of our survey questionnaire to 42 federal agencies that employ law enforcement officers about their use of the technology.¹ The report provides a detailed description of our scope and methodology.

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.

Background

Federal and Non-Federal Systems with Facial Recognition Technology

Federal law enforcement may use systems with facial recognition technology owned by their respective agencies. They may also use systems owned by other government entities, including federal, state, local, tribal, and territorial government entities. Moreover, federal law

¹GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, [GAO-21-518](#) (Washington D.C.: June 3, 2021). Our June 2021 report was a public version of a sensitive report that we issued in April 2021 (GAO-21-243SU). Some federal agencies deemed information in our April 2021 report to be sensitive, which must be protected from public disclosure. Therefore, the June 2021 report and this statement omit sensitive information about federal agency ownership and use of facial recognition technology.

enforcement may use non-government facial recognition service providers, such as Vigilant Solutions and Clearview AI. For example, law enforcement officers with a Clearview AI account may use a computer or smartphone to upload a photo of an unknown individual to Clearview AI's facial recognition system. The system can return search results that show potential photos of the unknown individual, as well as links to the site where the photos were obtained (e.g., Facebook).

In some cases, law enforcement officers can access another entity's system and conduct a facial recognition search. Alternatively, law enforcement officers can request that another entity use its system to conduct facial recognition searches on their behalf. For example, federal law enforcement officers may ask a state police department to conduct facial recognition searches on their behalf.

Privacy Laws and Rules

Several statutory requirements govern the protection of personal information by federal agencies, including federal law enforcement's use of facial images. The Privacy Act of 1974 places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records (e.g. photos). According to Office of Management and Budget (OMB) officials, the Privacy Act and OMB Circular A-130 generally provide that agencies must ensure that privacy requirements apply to systems operated by contractors or other entities on behalf of the Federal Government, which could include facial recognition service providers.

Accuracy of Facial Recognition Technology

The accuracy of facial recognition technology can be characterized in a number of ways. For example, a false positive rate is how often the technology incorrectly declares two images to be a match when they are actually from two different people. In addition, a false negative rate is how often the technology fails to declare two images to be a match when they are actually from the same person. Matching errors can be caused not only by the quality of the facial recognition technology, but also by the quality of the photos used in the matching process and other factors. The National Institute of Standards and Technology has conducted research into the accuracy of facial recognition algorithms. It has evaluated hundreds of commercial facial matching algorithms for accuracy and speed since 2000.

Twenty Federal Agencies Reported Owning or Using Systems with Facial Recognition Technology

We surveyed 42 federal agencies that employ law enforcement officers, 20 of which reported that they owned a system with facial recognition technology or used another entity's system.² As shown in figure 1, three agencies only owned a system, 12 agencies only used another entity's system, and five agencies both owned a system and used another entity's system. According to these agencies, some systems can include hundreds of millions or billions of photos.

²Specifically, we asked agencies whether at any point from January 2015 through March 2020, they owned a system with facial recognition technology, including systems in the process of being developed. In addition, we asked agencies whether at any point from April 2018 through March 2020, they used facial recognition technology—that is, their offices, employees, or contractors (1) accessed a system owned/operated by another entity, or (2) requested that another entity use its system to conduct a facial recognition search on their behalf. See the complete list of 42 federal agencies that received our questionnaire in appendix I.

We defined facial recognition technology as a type of automated or semi-automated biometric technology that uses images for verification, identification, and/or investigative purposes. In addition, we stated that a system with facial recognition technology may include a facial recognition algorithm, hardware, software, and a photo database. We asked agencies to include all uses of facial recognition technology in their response except for facial recognition technology that was solely used to authenticate the identity of the agency's employees and contractors to log into computers and phones.

Figure 1: Ownership and Use of Facial Recognition Technology Reported by Federal Agencies that Employ Law Enforcement Officers

Owned system	Used another entity's system			Owned system and used another entity's system	
					
Department of Veterans Affairs Police Service	Bureau of Alcohol, Tobacco, Firearms, and Explosives	Bureau of Diplomatic Security	Drug Enforcement Administration	U.S. Customs and Border Protection	Federal Bureau of Investigation
					
Federal Bureau of Prisons	Food and Drug Administration, Office of Criminal Investigations	U.S. Fish and Wildlife Service	U.S. Immigration and Customs Enforcement	Pentagon Force Protection Agency	U.S. Secret Service
					
National Aeronautics and Space Administration, Office of Protective Services	Internal Revenue Service, Criminal Investigation Division	U.S. Capitol Police	U.S. Marshals Service	Transportation Security Administration	
					
	U.S. Park Police	U.S. Postal Inspection Service	U.S. Probation and Pretrial Services		

Source: GAO analysis of survey data. | GAO-21-105309

Note: We sent a survey questionnaire to 42 federal agencies that employ law enforcement officers. We asked agencies whether at any point during January 2015 through March 2020, they owned a system with facial recognition technology, including systems in the process of being developed. In addition, we asked agencies whether at any point from April 2018 through March 2020, they used facial recognition technology—that is, their offices, employees, or contractors (1) accessed a system owned or operated by another entity, or (2) requested that another entity use its system to conduct a facial recognition search on their behalf.

The owned system columns include systems in the process of being developed. The National Aeronautics and Space Administration's Office of Protective Services reported that it did not purchase facial recognition technology. However, we included the agency in the owned column because it used a commercial-off-the-shelf product with facial recognition technology to conduct a proof of concept test to determine whether the technology was suitable for its purposes.

Eight Agencies Reported Owning Systems with Facial Recognition Technology

Eight of the 42 federal agencies reported owning 17 systems with facial recognition technology, from January 2015 through March 2020.³ Of these systems, four were in operation as of March 31, 2020, and were owned by three agencies: the Federal Bureau of Investigation, Federal Bureau of Prisons, and U.S. Customs and Border Protection. In addition, one of the eight agencies reported that it was in the process of procuring two systems during this time period, but had not finalized the purchase as of March 2020. Detailed descriptions of the 19 systems (17 owned and two in procurement) and their status as of March 31, 2020 can be found in our June 2021 report.

Seventeen Federal Agencies Reported Using Systems Owned by Other Entities

Seventeen of the 42 federal agencies reported using another entity's system with facial recognition technology from April 2018 through March 2020. Of the 17 agencies, 15 reported using systems owned by another federal entity; 14 reported using systems owned by state, local, tribal, or territorial entities; and 11 reported using systems owned by non-government entities. Furthermore, nine of the 17 agencies reported using systems owned by all three types of entities. See table 1 for additional information.

Table 1: Reported Use of Other Entities' Facial Recognition Technology by Federal Agencies that Employ Law Enforcement Officers

Federal Agency That Used System	Type of Entity That Owned System				
	Other Federal	State, Local, Tribal, Territorial	Non-Government ^a		
			Clearview AI	Vigilant Solutions	Other Non-Government ^b
Bureau of Diplomatic Security	✓	✓	✓	✓	✓
U.S. Customs and Border Protection	✓	✓	✓	✓	✓
U.S. Marshals Service	✓	✓	✓	✓	✓
Bureau of Alcohol, Tobacco, Firearms and Explosives	✓	✓	✓	✓	—
U.S. Immigration and Customs Enforcement	✓	✓	✓	—	✓

³This statement omits some information about systems owned by agencies we surveyed, as the relevant agencies deemed the information sensitive.

Federal Agency That Used System	Type of Entity That Owned System				
	Other Federal	State, Local, Tribal, Territorial	Non-Government ^a		
			Clearview AI	Vigilant Solutions	Other Non-Government ^b
U.S. Postal Inspection Service	✓	✓	✓	✓	—
Drug Enforcement Administration	✓	✓	✓	—	—
Federal Bureau of Investigation	✓	✓	✓	—	—
U.S. Secret Service	✓	✓	✓	—	—
U.S. Capitol Police	✓	✓	—	—	—
U.S. Fish and Wildlife Service	✓	✓	—	—	—
Food and Drug Administration, Office of Criminal Investigations	✓	✓	—	—	—
Internal Revenue Service, Criminal Investigation Division	✓	✓	—	—	—
U.S. Park Police	—	✓	✓	—	—
Administrative Office of the U.S. Courts, U.S. Probation and Pretrial Services	—	—	—	—	✓
Pentagon Force Protection Agency	✓	—	—	—	—
Transportation Security Administration	✓	—	—	—	—
Total	15	14	10	5	5

Legend:

✓ Agency used a system owned by the respective entity (or entity type) at any point from April 2018 through March 2020. For federal, state, local, tribal, and territorial entities, the term "used" includes an agency's offices, employees, or contractors (1) accessing a system owned/operated by the respective entity type, or (2) requesting that the respective entity type use its system to conduct a facial recognition search on the agency's behalf. For non-government entities, the term "used" means the agency's offices, employees, or contractors submitted photos to the respective non-government service provider for the purpose of conducting a facial recognition search.

— Agency did not use a system owned by the respective entity (or entity type) at any point from April 2018 through March 2020.

Source: GAO analysis of survey data. | GAO-21-105309

^aSome agencies reported that they only used Clearview AI or Vigilant Solutions on a free trial basis, and thus, did not enter into a formal contract with the service provider.

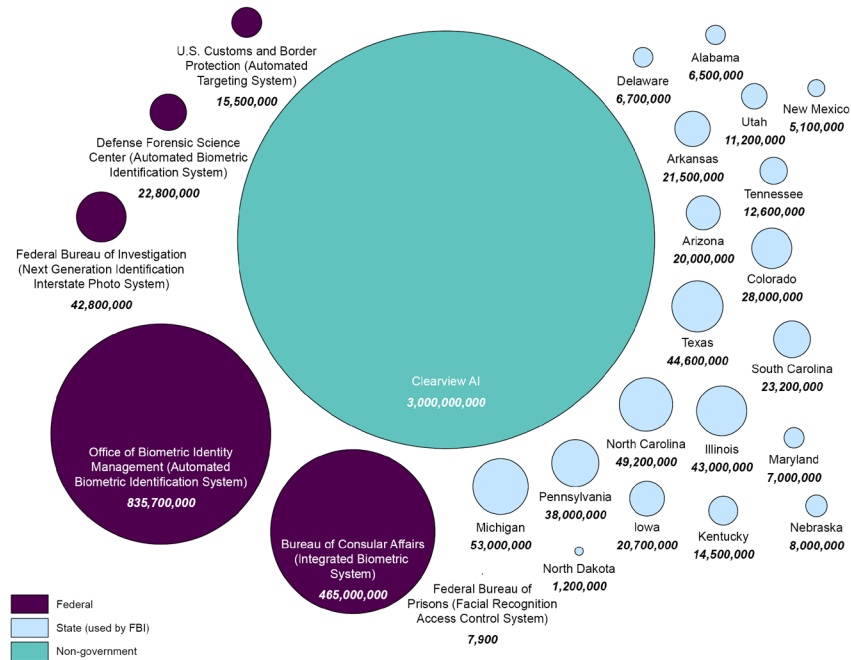
^bOther non-government entities that agencies reported using included Amazon Rekognition, BI SmartLink, and Giant Oak Social Technology, among others.

Agencies Reported Using Systems that Varied in the Number and Type of Photos

Federal agencies reported using numerous systems with facial recognition technology, and sometimes these systems included stored photos. The number and types of photos within these systems can vary, based on information reported by agencies and system owners. Reported photo types included: mug shot photos, driver's license photos, passport photos, publicly available photos on the internet, and images from video/Closed Circuit Television. Figure 2 below shows examples of federal, state, and non-government systems with facial recognition

technology that federal agencies reported using, and the number of photos in them.

Figure 2: Selected Federal, State, and Non-government Systems with Facial Recognition Technology Used by Federal Agencies that Employ Law Enforcement Officers, and the Number of Photos in Them



Note: We sent a survey questionnaire to 42 federal agencies that employ law enforcement officers. This figure includes examples of systems used by one or more federal agencies we surveyed. It does not include all systems used by these agencies. The figure includes the number of photos stored in the respective entity's system with facial recognition technology, as of March 31, 2020.

The same individual may be included in multiple photos within one photo database or across multiple databases, and the same photo can exist within multiple databases. Some entities providing these numbers indicated they were estimates. The number of photos for federal and non-government entities were reported by the respective system owner. The number of photos for state entities were all reported by the Federal Bureau of Investigation (FBI). Specifically, the FBI's Facial Analysis, Comparison, and Evaluation Services has memorandums of understanding with several state agencies, allowing it to leverage the state-owned systems for facial recognition searches. The FBI provided the number of photos they can access via these memorandums of understanding.

Federal Agencies Reported Using Systems with Facial Recognition Technology to Support Various Activities

Federal agencies reported using facial recognition technology to support various activities, such as criminal investigations and surveillance, and also in response to the Coronavirus Disease 2019 (e.g., verify an individual's identity remotely). Of the 20 agencies that owned or used facial recognition technology, 14 reported using the technology to support criminal investigations. For example, the FBI's Next Generation Identification Interstate Photo System allows users to search a database of over 40 million photos. The system returns a list of potential candidates that law enforcement can use to generate investigative leads. According to the FBI, the system has been used for investigations of violent crimes, credit card and identity fraud, missing persons, and bank robberies, among others.

Six agencies reported using facial recognition technology during May through August 2020 to support criminal investigations related to civil unrest, riots, or protests.⁴ Following the killing of Mr. George Floyd while in the custody of the Minneapolis, Minnesota police department on May 25, 2020, nationwide civil unrest, riots, and protests occurred. Six agencies told us that they used images from these events to conduct facial recognition searches during May through August 2020 in order to assist with criminal investigations (see table 2). All six agencies reported that these searches were on images of individuals suspected of violating the law.

⁴We requested this information from 17 agencies that indicated in their questionnaire response as (1) having a system with facial recognition technology that was in operation, or (2) using another entity's system.

Table 2: Federal Agency Reported Use of Facial Recognition Technology on Images of Individuals Suspected of Violating the Law during Civil Unrest, Riots, or Protests, May through August 2020

Federal Agency	How Agency Reported Using Facial Recognition Technology
Bureau of Alcohol, Tobacco, Firearms and Explosives	In a single instance, used facial recognition technology owned by another law enforcement entity. The search was conducted to help identify an individual suspected of violating the law during the period of civil unrest, riots, or protests.
U.S. Capitol Police	Requested that the Montgomery County Department of Police (Montgomery County, Maryland) conduct facial recognition searches to assist with a criminal investigation. The purpose of the searches was to help identify individuals that confronted and made threats to a member of Congress and the member's spouse outside the White House during the period of civil unrest, riots, or protests.
Federal Bureau of Investigation	Created a digital media tip line and solicited images of people involved in criminal activity during the period of civil unrest, riots, or protests. The agency sought to identify or locate criminal suspects seen in images and video depicting criminal behavior by conducting facial recognition searches using its Next Generation Identification Interstate Photo System.
U.S. Marshals Service	Used a non-government facial recognition service provider to conduct facial recognition searches related to criminal investigations on images from the period of civil unrest, riots, or protests.
U.S. Park Police	Requested that the Maryland National Capital Park Police conduct a facial recognition search using an image from Twitter to identify an individual who allegedly assaulted an officer during the period of civil unrest, riots, or protests. The search was conducted on the National Capital Region Facial Recognition Investigative Leads System. The subject was ultimately charged with Felony Civil Disorder and two counts of Assault on a Police Officer.
U.S. Postal Inspection Service	Used Clearview AI to help identify individuals suspected of criminal activity that took place in conjunction with the period of civil unrest, riots, or protests. This criminal activity included damaging U.S. Postal Service property, stealing mail, opening mail, burglarizing U.S. Postal Service buildings, and committing arson.

Source: GAO analysis of survey data | GAO-21-105309

Three agencies reported using facial recognition technology on images from the U.S. Capitol attack on January 6, 2021.⁵ The three agencies reported using the technology to generate investigative leads for criminal investigations as follows:

- U.S. Capitol Police used Clearview AI to help generate investigative leads. The agency also requested that another federal agency use its system to conduct facial recognition searches on behalf of the U.S. Capitol Police.

⁵We asked agencies whether they used facial recognition on images of the civil unrest, riots, or protests at the U.S. Capitol complex on January 6, 2021. We requested this information from 17 agencies that indicated in their questionnaire response as (1) having a system with facial recognition technology that was in operation, or (2) using another entity's system. See more information on our methodology in appendix I in [GAO-21-518](#). Twelve agencies reported that they did not use the technology for these purposes, three agencies reported using the technology, and two agencies told us they could not answer our questions because the information pertains to ongoing investigations.

- U.S. Customs and Border Protection used its Automated Targeting System to conduct searches at the request of another federal agency.
- Bureau of Diplomatic Security used the Department of State's Integrated Biometric System to conduct searches at the request of another federal agency.

Agencies also reported using facial recognition technology to support other activities, such as surveillance, traveler verification, area access, and research and education. For example, the U.S. Secret Service piloted a system with facial recognition technology to determine whether it could be incorporated into the agency's White House Complex security operations. Specifically, the Secret Service stored photos of 23 volunteer employees within the system. As volunteers moved throughout the White House Complex, their images were captured by closed-circuit television cameras. In real time, the system compared the stored photos to images from the video footage to determine whether they represented the same individual. Secret Service told us it did not plan to implement the system based on the results of the pilot.

Most Agencies Do Not Track Non-Federal Systems in Use or Related Risks

Thirteen agencies do not have complete, up-to-date information on what non-federal systems are used by employees.⁶ These 13 agencies have therefore not fully assessed the potential risks of using these systems, such as risks related to privacy and accuracy. Most federal agencies that reported using non-federal systems did not own systems. Thus, employees were relying on systems owned by other entities, including non-federal entities, to support their operations.

Specifically, we found that 13 of 14 agencies that reported using non-federal systems do not have a mechanism to track what non-federal systems are used by employees (see table 3).⁷ For example, when we requested information from one of the agencies about its use of non-federal systems, agency officials told us they had to poll field division personnel because the information was not maintained by the agency. These agency officials also told us that the field division personnel had to

⁶By complete, up-to-date information, we mean that an agency has ongoing knowledge of what non-federal systems with facial recognition technology are used by employees. By non-federal systems, we are referring to systems owned by state, local, tribal, territorial, and non-government entities.

⁷Fifteen agencies reported using non-federal systems; however, we excluded U.S. Probation and Pretrial Services because it does not use facial recognition technology to support criminal investigations. All 14 agencies discussed in this section reported using the technology to support criminal investigations.

work from their memory about their past use of non-federal systems, and that they could not ensure we were provided comprehensive information about the agency's use of non-federal systems. Officials from another agency initially told us that its employees did not use non-federal systems; however, after conducting a poll, the agency learned that its employees had used a non-federal system to conduct more than 1,000 facial recognition searches.

Table 3: Tracking of Employee Use of Non-Federal Systems with Facial Recognition Technology among Selected Federal Agencies

Federal Agency	Have Mechanism to Track What Non-Federal Systems Are used by Employees
U.S. Immigration and Customs Enforcement	Yes
Bureau of Alcohol, Tobacco, Firearms and Explosives	No
Bureau of Diplomatic Security	No
U.S. Capitol Police	No
U.S. Customs and Border Protection	No
Drug Enforcement Administration	No
Federal Bureau of Investigation	No
U.S. Fish and Wildlife Service	No
Food and Drug Administration, Office of Criminal Investigations	No
Internal Revenue Service, Criminal Investigation Division	No
U.S. Marshals Service	No
U.S. Park Police	No
U.S. Postal Inspection Service	No
U.S. Secret Service	No

Source: GAO analysis of agency information. | GAO-21-105309

Note: Federal agencies marked "No" may have known that employees used certain systems, but they do not have a mechanism to provide complete, up-to-date information of what systems are used by employees.

Numerous risks to federal agencies and the public can accompany the use of facial recognition technology. In particular, these risks can relate to privacy and the accuracy of a system. For example, when agencies use facial recognition technology without first assessing the privacy implications, there is a risk that the agencies will not adhere to privacy-related laws, regulations, and policies. There is also a risk that non-federal system owners will share sensitive information (e.g. photo of a suspect) about an ongoing investigation with the public or others.

Although the accuracy of facial recognition technology has increased dramatically in recent years, risks still exist that searches will provide inaccurate results. For example, if a system is not sufficiently accurate, it could unnecessarily identify innocent people as investigative leads. The system could also miss investigative leads that could otherwise have been revealed. In December 2019, the National Institute of Standards and Technology reported that facial recognition algorithms it tested differed in accuracy widely by race, ethnicity, or country of origin, as well as by gender and age.⁸ Some members of Congress, privacy groups, and others have expressed concerns that facial recognition technology's higher error rates for certain demographics could result in disparate treatment, profiling, or other adverse consequences for members of these populations.

One agency—the U.S. Immigration and Customs Enforcement—reported that it was in the process of implementing a mechanism to track what non-federal systems are used by employees. According to U.S. Immigration and Customs Enforcement officials, in November 2020 they were in the process of developing a list of approved facial recognition technologies that employees can use. In addition, log-in sheets will be made available to employees, allowing supervisors to monitor employee use of the technologies. The agency also assessed privacy and accuracy risks associated with its use of facial recognition technology, including non-federal systems.⁹

However, 13 federal agencies cannot fully assess the risks of using non-federal systems because they do not have complete, up-to-date information on what systems are actually used by employees. Therefore, in June 2021 we recommended that these 13 agencies: (1) implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities; and (2) after implementing a mechanism to track non-federal systems, assess

⁸National Institute of Standards and Technology, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NIST Interagency or Internal Report 8280 (Dec. 19, 2019). The National Institute of Standards and Technology reported that it tested 189 mostly commercial algorithms from 99 developers and that performance differences varied by the algorithms tested, with some performing better than others. For a small number of the one-to-many algorithms, differences in false positives across demographic groups were undetectable. The extent of performance differences varied by the developer, type of error, and quality of the facial images.

⁹Department of Homeland Security, Privacy Impact Assessment for the ICE Use of Facial Recognition Services, DHS/ICE/PIA-054 (May 13, 2020).

the risks of using such systems, including privacy and accuracy-related risks.¹⁰

These agencies generally concurred with our recommendations.¹¹ We believe that expeditious implementation of our recommendations is essential. By implementing a mechanism to track what non-federal systems are used by employees, agencies will have better visibility into the technologies they rely upon to conduct criminal investigations. In addition, by assessing the risks of using these systems, including privacy and accuracy-related risks, agencies will be better positioned to mitigate any risks to themselves and the public.

Chair Jackson Lee, Ranking Member Biggs, and Members of the Subcommittee, this concludes my prepared statement. I would be pleased to respond to any questions you may have at this time.

GAO Contact and Staff Acknowledgements

If you or your staff have any questions about this testimony, please contact Gretta L. Goodwin, Director, Homeland Security and Justice, at (202) 512-8777 or GoodwinG@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Jeffrey Fiore (Assistant Director), Andrea Bivens (Analyst-In-Charge), Jennifer Beddor, Emily Flores, Richard Hung, Jason Jackson, Heidi Nielson, Erin Pineda, and Adam Schrier. Key contributors for the previous work that this testimony is based on are listed in the previously issued product.

¹⁰We made these recommendations to all 13 agencies that reported "No" in table 3 above.

¹¹As of June 2021, the 13 federal agencies have not implemented these recommendations.

Appendix I: Federal Agencies That Participated in GAO's Survey Questionnaire on Facial Recognition Technology

Our June 2021 report included the results of a survey questionnaire we sent to 42 federal agencies that employed law enforcement officers.¹ The survey focused on agency ownership and use of facial recognition technology. See the list of 42 federal agencies in table 4 below.

Table 4: Federal Agencies That Participated in GAO's Survey Questionnaire on Facial Recognition Technology

Federal Agency	Department
Forest Service	Agriculture
Bureau of Industry and Security	Commerce
National Oceanic and Atmospheric Administration, Office of Law Enforcement	Commerce
Office of Security	Commerce
Secretary's Protective Detail	Commerce
Pentagon Force Protection Agency	Defense
National Nuclear Security Administration	Energy
Food and Drug Administration, Office of Criminal Investigations	Health and Human Services
National Institutes of Health, Division of Police	Health and Human Services
U.S. Customs and Border Protection	Homeland Security
Federal Emergency Management Agency, Mount Weather Police	Homeland Security
Federal Protective Service	Homeland Security
U.S. Immigration and Customs Enforcement	Homeland Security
Office of the Chief Security Officer	Homeland Security
U.S. Secret Service	Homeland Security
Transportation Security Administration	Homeland Security
Bureau of Indian Affairs, Office of Justice Services	Interior
Bureau of Land Management	Interior
Bureau of Reclamation	Interior
U.S. Fish and Wildlife Service	Interior
U.S. Park Police	Interior
National Park Service Rangers	Interior
Bureau of Alcohol, Tobacco, Firearms, and Explosives	Justice
Drug Enforcement Administration	Justice
Federal Bureau of Investigation	Justice
Federal Bureau of Prisons	Justice

¹GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, [GAO-21-518](#) (Washington D.C.: June 3, 2021). In our June 2021 report, we defined federal law enforcement officers as full-time employees with federal arrest authority and who are authorized to carry firearms while on duty. See more information on our scope and methodology in our June 2021 report.

**Appendix I: Federal Agencies That Participated
in GAO's Survey Questionnaire on Facial
Recognition Technology**

Federal Agency	Department
U.S. Marshals Service	Justice
Division of Protective Operations	Labor
Bureau of Diplomatic Security	State
Bureau of Engraving and Printing Police	Treasury
Internal Revenue Service, Criminal Investigation Division	Treasury
U.S. Mint Police	Treasury
Police Service	Veterans Affairs
Amtrak Police Department	—
Environmental Protection Agency, Criminal Investigation Division	—
National Aeronautics and Space Administration, Office of Protective Services	—
U.S. Postal Inspection Service	—
Smithsonian Institution, Office of Protection Services	—
Tennessee Valley Authority Police	—
Administrative Office of the U.S. Courts, U.S. Probation and Pretrial Services	—
U.S. Capitol Police	—
Government Publishing Office, Uniform Police Branch	—

Legend: — Not Applicable

Source: GAO information. | GAO-21-105309

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on Facebook , Flickr , Twitter , and YouTube . Subscribe to our RSS Feeds or Email Updates . Listen to our Podcasts . Visit GAO on the web at https://www.gao.gov .
To Report Fraud, Waste, and Abuse in Federal Programs	Contact FraudNet: Website: https://www.gao.gov/about/what-gao-does/fraudnet Automated answering system: (800) 424-5454 or (202) 512-7700
Congressional Relations	Orice Williams Brown, Managing Director, WilliamsO@gao.gov , (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov , (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548
Strategic Planning and External Liaison	Stephen J. Sanford, Managing Director, spel@gao.gov , (202) 512-4707 U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548



Please Print on Recycled Paper.

Ms. JACKSON LEE. Thank you for your testimony.
I am now pleased to recognize Professor Barry Friedman for five minutes.

STATEMENT OF BARRY FRIEDMAN

Mr. FRIEDMAN. Chair Jackson Lee, Chair Nadler, Ranking Members Jordan and Biggs, Members of the Subcommittee, I want to thank you for giving me the opportunity to testify today.

As my introduction indicated, I am the founding director of the Policing Project at New York University School of Law. I want to tell you our mission because it relates directly to what you're doing today.

We are an organization that partners with all stakeholders. We work in impacted communities, communities impacted by law enforcement, we also work closely with law enforcement agencies, with the goal of bringing to policing democratic accountability, transparency, and equity, particularly around issues of race.

I want to stress two parts of that because I think they relate directly to this hearing.

First, the issue of democratic accountability. It's our position—this is one my key points that I'd like to make today—that these technologies should not be used without proper democratic accountability. Accordingly, I commend this Subcommittee for having this hearing to pursue what I think is essential legislation in this area.

Second, I want to stress that we do work with all stakeholders across the ideological spectrum. I was incredibly gratified to listen to all the Members who spoke to the need and the ability to work in a bipartisan way on this issue.

I believe that there are strong, passionate feelings about this technology. It's very powerful technology. There is a way forward on the technology, and the question is, how do we get there? So, I want to turn to that.

The approach that we use at the Policing Project, particularly for emerging technologies around policing, is one of cost-benefit analysis.

We look at the benefits of the technology. As many of you said, there are definitely benefits that can be obtained from this technology.

Then we look at the costs. As many of you have indicated, there are very, very serious costs, very, very serious potential harms. There are racial harms from the disparities. There are privacy harms. There are harms of giving too much power to governments, as we can all see by use of this technology by totalitarian governments. There are concerns about the First Amendment.

Now, some people look at cost-benefit analysis and they think, okay, well, we weigh the costs, we weigh the benefits, we decide whether to do something or not.

That's exactly the wrong approach. The value of cost-benefit analysis or benefit-cost analysis is that we can find a nuanced way to regulate that can maximize the benefits and minimize or mitigate entirely the harms. That's what I want to talk about.

I have spoken to many, many people over the last months and, in fact, years about this issue. There are strong views on both

sides, including some people who after much reason think that the technology should be banned.

The fact of the matter is that when I am talking to law enforcement or when I am talking to civil libertarians or racial justice advocates, whether I am talking about to people in the technology companies themselves, even though they disagree about the use of the technology and about many things, there's a wide swath of agreement about what isn't okay in the use of the technology, about what are shoddy and dangerous practices that should be regulated.

I want to just dive very quickly into some of the nuance of those practices, and you have a longer enumeration in my testimony, and I am happy to answer any questions.

So, first, issues of accuracy and bias. We've heard a lot about that. I think it's time, and I hope that we will all stop saying things like the technology is 87, 93, or 95 percent accurate. That doesn't mean anything. We should be talking about false negatives and false positives. That's what matters.

The truth of the matter is we don't know anything about the accuracy of this technology when law enforcement uses it. That is because law enforcement uses the technology in a way different than it has been tested by NIST. Law enforcement uses different probe images than NIST has tested. Law enforcement uses much larger databases than NIST has tested. As you think about it, the error rates just increase as the databases get larger. We don't even know if NIST has tested the actual algorithms that law enforcement is using.

Now, a lot of people say, "Okay. Not to worry. There's a human in the loop." Now, I would appeal to your common sense. We don't have enough science, but we have some. Humans in the loop can be a good thing or a bad thing.

Humans in the loop would be a good thing if an independent individual who had no idea what the algorithm had suggested identified the same person.

Humans in the loop are problematic if all they're doing is confirming what the algorithm told them.

So, again, we need testing and methods of ensuring that if there's a human in the loop, that human is actually working in a way to make sure that we eliminate concerns about accuracy and demographic—particularly racial—bias.

Finally, I want to urge you to think very seriously about regulating the vendors themselves. That's the touch point. Those are the folks that know how the technology works and what can be done to make it work. They could work on what are acceptable probe photos, what are the right settings to make sure we get accurate results.

I have a long list of things the vendors could regulate, but I am out of time. So, I am just going to thank you for listening to my testimony, and I am happy to answer questions.

[The statement of Mr. Friedman follows:]

**Written Testimony of Barry Friedman
Jacob D. Fuchsberg Professor of Law and
Associated Professor of Politics;
Faculty Director, Policing Project
New York University School of Law**

Before the House Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security
Facial Recognition Technology: Examining Its Use by Law Enforcement
July 13, 2021

Chairwoman Jackson Lee, Chairman Nadler, Ranking Member Jordan, Ranking Member Biggs and Distinguished Members of the Subcommittee: Thank you for inviting me to testify on the topic of the use of facial recognition technology by law enforcement.

In my remarks today, I would like to make three overarching points:

- (1) Facial recognition technology (FRT), especially in the hands of law enforcement, is an extremely powerful tool; and it can be powerful for good and for bad;
- (2) The present lawless status quo around law enforcement's use of FRT is unacceptable: there is an urgent need for comprehensive, nuanced regulation that would allow obtaining the benefits of this technology for public safety while eliminating the harms, in particular harms to marginalized communities—and especially Black communities—which bear the brunt of FRT harms at present; and
- (3) I want to highlight key considerations that should be included in any regulatory approach to FRT, including steps Congress can take right now to rein in the risks posed by law enforcement's ongoing use of this technology.

I. Background for testimony

I am the Jacob D. Fuchsberg Professor of Law and Affiliated Professor of Politics at New York University School of Law. For over thirty years I have taught a number of courses relevant to this hearing, including Constitutional Law, Criminal Procedure, and Democratic Policing. I also am the author of numerous publications, in both the scholarly and public realm, about regulating policing, including *Unwarranted: Policing Without Permission*.

Perhaps most germane, I also am the Faculty Director of the Policing Project at NYU Law School. Our mission is to “partner with communities and police to promote public safety through transparency, equity, and democratic engagement.”¹ We conduct research, but also do work on the ground all over the country, both with policing agencies and the communities they serve, to promote democratically-accountable policing. Ours is an all-stakeholders approach. Everywhere we work, we endeavor to do so both with communities affected by policing, and with the police themselves. That is reflected in our [Advisory Board](#), which surely is unique in including public officials, activists, policing leaders, and civil liberties and racial justice advocates, among others. By listening to, and working with, everyone we hope to move the needle toward greater public safety that is just, non-discriminatory, and effective. If you are interested in the full scope of our work, you can learn more at our website, www.policingproject.org.

One of our primary areas of study and work is the use of emerging technologies by law enforcement. And core to that is facial recognition. I think it is fair to say I have spent hours and hours in discussion about these issues with law enforcement, with members of impacted communities, with racial justice and civil liberties advocates, and with representatives of the technology companies that make these products. Always looking for a sensible way forward to what is a very real and pressing social problem.

¹ *Our Mission*, Policing Project, <https://www.policingproject.org/our-mission>

II. The need for “front-end accountability”

Hearings like this are at the core of the Policing Project’s mission. To explain why that is, I would like to draw an important distinction between what we refer to as “front-end” and “back-end” accountability.

There has been a great deal of concern in the country over the last few years about the impact of policing. Some of that concern has been about uses of force and coercion, be it police shootings or pedestrian and traffic stops. But it also has been about the kinds of technology you seek to address here, like facial recognition. And when these issues are discussed, the word “accountability” often is used.

But there are two kinds of accountability and they are very different. Most of what we hear about in policing is “back-end accountability.” The police have done something that people feel is wrong, and they want to assign responsibility and see that there is responsive action taken. Examples include proceedings in court to exclude evidence that is obtained unlawfully, or the prosecution of officers, federal investigations or civil rights suits, and the like. All these are aimed at accountability after-the-fact, after something has happened. Back-end accountability is essential, but because it only targets misconduct, there is a limit to what it can accomplish to guide policing before it goes awry.

What has been almost entirely missing from policing is accountability of a very, very different sort: front-end accountability. By that I mean to say that the public has a voice in setting transparent, ethical, and effective policing policies *before* the police or government act. The very work you as legislators do daily. Although we expect this in most areas of government, policing is a striking exception.

In my view, the lack of democratic front-end accountability explains many of the problems with policing today. Take facial recognition as an example. Policing agencies have acquired and used this technology in secretive ways, without adequate guardrails around use cases or means of use. People are distrustful when surveillance technologies are used without transparency and rules. This is only natural. And nowhere is the mistrust higher than in Black and brown and marginalized communities, which already feel the brunt of many unfortunate policing practices. The wise policing leaders I know understand they cannot fight crime or achieve public safety without community trust. And if there is going to be trust around surveillance technologies—especially in the communities understandably most distrustful of policing at present, there has to be great sensitivity to the issues that lead to such mistrust. That means complete transparency, and a regulatory approach that recognizes and addresses harms.

But frankly, it is asking too much of policing agencies to develop regulatory approaches to complex technologies on their own. That is the job of legislative bodies. It is your job. This hearing is a great example of front-end accountability in action, and I am grateful for the opportunity to participate.

III. There is an urgent need to regulate law enforcement use of FRT

Of all the new technologies used by policing agencies today, none has captured the public’s attention as intently as facial recognition technology. This is not surprising – unlike some other modern crime-fighting tools such as cell-site simulators or even other biometrics such as DNA – its utility is intuitive and nightmare scenarios of government misuse are not hard to imagine. We don’t even have to imagine them: one need only look to FRT’s use for state-sanctioned mass

surveillance and social control in China and Russia, including of racial minorities such as the Uyghurs.² Put simply, the power of this technology, and the threat it poses, is obvious and real.

At the same time, there is promise in the technology. That is why law enforcement has embraced it so quickly. It provides a way to identify people quickly including suspects in criminal offenses, or locating subjects of Amber and Silver alerts. Federal agencies have used FRT to identify individuals who entered the Capitol unlawfully on January 6, 2021.

Too often, the use of new technologies by police is debated as a matter of being “for” or “against” it. We become highly polarized. At the Policing Project, we believe the better approach is to figure out if society can benefit from a particular technology. Then, if there are real benefits to be had, the question becomes whether it is possible to minimize or eliminate any harm. And we have to pay special and close attention to where those harms fall. Too often, society sees a net benefit in some policing practice, and pays little attention to the fact that the harms fall on particular communities—especially BIPOC communities. That is flat out unacceptable. Addressing crime and achieving public safety only works if it is co-produced by police and the community, and that will not happen when the costs of policing fall disproportionately on some communities.

I often have heard proponents of this technology in the law enforcement community and beyond argue that FRT is just another tool in the police tool belt, or that it’s just a more efficient way of doing the same thing police always do when trying to identify a suspect, victim or witness: i.e., sort through mugshots. This is not true. With FRT, police can (and do) search databases of millions of faces in a matter of seconds. AI-driven tools of this sort offer police the ability to sort, organize, and store unfathomably large quantities of our personal information, and to track people wherever they go. In short, as the Supreme Court and legal scholars have recognized, when it comes to surveillance technologies used by police, “digital is different.”³

The problem we face is that today in too many jurisdictions the use of this technology is entirely unregulated, and with a lack of regulation comes harm. Although a few states recently have passed legislation addressing law enforcement use of this technology, the status quo for most of the country remains a regulatory vacuum.⁴ This is untenable. Some agencies may use FRT wisely; some agencies are doing just the opposite. It is the Wild West out there, and you have the authority to address this problem. Until there is a real, comprehensive regulatory regime for FRT, there will be misuse, and mistrust. The technology simply should not be in use—other than perhaps controlled experiments from which we can learn—until a regulatory framework is in place.

There is no hiding from the fact that true regulation of FRT presents complicated issues. What we need is careful study and rational regulation. Indeed, it is imperative, because we should not kid ourselves: FRT is just one of many biometric technologies in the product development

² See, e.g., Alfred Ng, *How China uses facial recognition to control human behavior*, CNET (Aug. 11, 2020), <https://www.cnet.com/news/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/>; Robyn Dixon, *Russia’s surveillance state still doesn’t match China. But Putin is racing to catch up*, WASH. POST (Apr. 17, 2021), https://www.washingtonpost.com/world/europe/russia-facial-recognition-surveillance-navalny/2021/04/16/4b97dc80-8c0a-11eb-a33e-da28941cb9ac_story.html.

³ E.g., Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1128-29 (2021); Jennifer Stisa Granick, *SCOTUS & Cell Phone Searches: Digital is Different*, JUST SECURITY (June 25, 2014), <https://www.justsecurity.org/12219/>.

⁴ E.g., An Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth, 2020 Mass. Acts ch. 253; An Act to Increase Privacy and Security by Prohibiting the Use of Facial Surveillance by Certain Government Employees and Officials, 2020 Me. Laws ch. 394; An Act Relating to the Use of Facial Recognition Services, 2020 Wash. Sess. Laws 1847.

pipeline. In the balance of my remarks, I will apply this benefit-cost approach to argue for nuanced regulation. As you will see, we are a long way off from that.

IV. Use cases

I want to distinguish among several very different use cases for FRT, as I think the analysis may differ across them. My remarks are directed at one particular use case: FRT for retrospective investigative identifications. By that I mean when law enforcement uses FRT to identify a person (or persons) by searching a still image—often called a “probe image”—against a database of other still images to return a list of candidates for comparison.⁵ (I will refer to the database against which a probe image is searched as the “enrollment database.”) I focus on the identification use case for two reasons: (1) it appears to be the most common way that law enforcement uses this technology at present; and (2) I believe it is the use case for which nuanced, comprehensive legislation is most apt.⁶

I distinguish this use case from two others – face verification and face surveillance. Face verification, the process of authenticating a person’s identity by comparing two images, also generally is used by law enforcement, in particular by U.S. border enforcement agencies to authenticate travelers’ identities.⁷ This use case is not without risks – and indeed should be subject to many of the same guardrails that I detail below for face identification. Yet two conditions make me less nervous about verification if subject to proper controls: first, leading face verification algorithms generally are more accurate and less biased than leading face identification algorithms.⁸ This is due at least in part to the fact that verification only requires comparing two images rather than images across an entire enrollment database, which is when the error rate gets compounded.⁹ Second, because face verification does not require creating databases that store annotated images of our faces, it can raise fewer privacy concerns.

On the other hand, FRT for face surveillance – i.e., using real time or stored video footage to track people as they pass by public or private surveillance cameras, allowing their whereabouts to be traced – raises such serious privacy and liberty concerns, I continue to think the risks of allowing it outweigh the benefits. At the least I would not consider allowing it unless and until we can prove our ability to regulate and control the use of FRT for face identification. And we certainly have not done that.

V. Evaluating the benefits and costs of FRT for face identification

It is not difficult to articulate the (at least intended) benefits of this use case: the ability to solve serious crimes more quickly and efficiently. Proponents of this technology are quick to offer

⁵ I use the term “identification” to reflect common parlance. In truth, a more precise way to conceive of the underlying process is that the algorithm actually is making a prediction about the likelihood that two images do or do not represent the same person.

⁶ Kristin Finklea et al., *Federal Law Enforcement Use of Facial Recognition Technology*, CONG. RESEARCH SERV. 5 (Oct. 27, 2020), <https://fas.org/sgp/crs/misc/R46586.pdf>.

⁷ *Id.* at 6.

⁸ Compare NIST FRVT 1:1 Verification, Verification Performance, <https://pages.nist.gov/frvt/html/frvt11.html> with NIST FRVT 1:N Identification, Identification Performance, <https://pages.nist.gov/frvt/html/frvt1N.html>; see also generally Patrick Grother et al., Nat’l Inst. Stds. & Tech., *NISTIR 8280: Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (2019).

⁹ Handbook of Face Recognition, 644 (Stan Z. Li & Anil K. Jain, eds., 2d ed. 2011).

up anecdotes of FRT used to aid investigations of child kidnapping or sex trafficking. These examples are real and I take seriously the claim about the value of FRT to advance public safety. We all should. Police officers face a laborious and often fruitless task when they try to match photos of crime suspects to mug shots of people who have already been arrested. And I do not have to belabor with this audience the utility that face recognition can offer in investigations of a mass attack, such as occurred in your halls on January 6th. There is also the potential benefit that, properly structured, FRT offers an opportunity to make the eyewitness identification process more objective and auditable. According to the Innocence Project, mistaken eyewitness identifications account for 69% of wrongful convictions that have been overturned by DNA evidence.¹⁰ FRT has the potential to help.

The problem with these benefits is we have little idea of their scope. We are left, as we are too often with policing, with nothing but anecdote. How many policing agencies are using FRT? How often has it been used successfully or unsuccessfully? How many identifications would have been made without FRT and at what expenditure of time? An economist would tell you that in doing benefit-cost analysis there is no need even to delve into costs until you are certain there are benefits. It simply is unacceptable that we plunge into the world of biometric face identification with no attempt whatsoever to know how valuable it is.

On the other hand, there are very real costs, especially social costs, to using the technology. I will review a few of them briefly; I have written about them extensively elsewhere, and others testifying today such as my friend Sakira Cook from the Leadership Conference will probe them at length.¹¹ First, there are significant accuracy and bias concerns that can have very serious racial impacts. This is not hypothetical. FRT is not now, nor will it ever be, perfect and many of even the best algorithms do not perform equally well across demographic groups. At present, many algorithms have higher error rates when attempting to identify individuals from certain marginalized groups, including people of color and women. Racial disparities are not unique to the algorithms; rather, they infect the entire process.¹² Disparities in arrest rates mean that the criminal databases that many agencies use for face recognition searches have a disproportionate number of Black, Latinx, and immigrant faces.¹³ In addition, enforcement disparities exist across many levels of the criminal system – from the rates of traffic and pedestrian stops, to arrest and incarceration rates. In particular, studies continue to show that enforcement of low-level and drug offenses disproportionately targets Black Americans.¹⁴ Comprehensive data on law enforcement use of FRT do not exist, but if its use tracks typical enforcement patterns, then communities of color likely are subject to more FRT searches. Indeed, before ending its program, San Diego found

¹⁰ *Eyewitness Identification Reform*, Innocence Project, <https://innocenceproject.org/eyewitness-identification-reform>.

¹¹ Barry Friedman, *Unwarranted: Policing Without Permission* 29–233 (2017).

¹² Like anyone who studies issues of accountability and racial bias in AI systems, we all owe a debt to the trailblazing work of Joy Buolamwini, Timnit Gebru, and Inioluwa Deborah Raji, among others. Their research, including *Gender Shades*, *Datasheets for Datasets and Model Cards for Model Reporting*, has taught us a great deal about the biases in FRT technologies and what must be done about them. See, e.g., Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, PMLR (2018); Timnit Gebru et al., *Datasheets for Datasets*, PMLR (2018); Margaret Mitchell et al., *Model Cards for Model Reporting*, ACM (2019).

¹³ Jennifer Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology*, EFF 10 (2020), https://www.eff.org/files/2020/04/20/face-off-report-2020_1.pdf.

¹⁴ See generally Elizabeth Hinton et al., *An Unjust Burden: The Disparate Treatment of Black Americans in the Criminal Justice System*, VERA INSTITUTE (2018), <https://www.vera.org/downloads/publications/for-the-record-unjust-burden-racial-disparities.pdf>.

that police used FRT up to 2.5 more times on communities of color as compared to their presence in the general population.¹⁵

Second, FRT poses a very real threat to privacy and autonomy. It should take no lengthy discussion to establish this. Whether it's our faces ending up in FRT databases solely because we want to operate a vehicle or fears of cameras that can track and identify us, the risks to individual privacy and autonomy have been written about extensively. The warm embrace of FRT by authoritarian regimes as a means of social control should give us pause.

Third, the availability of this technology can chill First Amendment freedoms. Both historical and current law enforcement practice shows this hardly is hypothetical, whether one refers to the notorious COINTELPRO efforts of law enforcement agencies during the civil rights era, or the recent conduct of various South Florida police agencies that ran images from Black Lives Matter protests and a Juneteenth Block Party through a massive, unregulated face recognition database.¹⁶ There is a persistent inclination of those in power to investigate and tamp down dissent. The Framers of our Constitution understood this all too well. And, unfortunately, these uses of surveillance tools also too frequently are aimed at marginalized communities.

Finally (although I am skipping over other harms), unlike almost every other form of forensic evidence, defendants rarely are informed that FRT was used in their case. This lack of disclosure could hamper the defense's ability to conduct a thorough investigation. For example, although it is standard to disclose other matches produced by traditional police lineups or photo arrays, this practice apparently does not apply to FRT results. And there remain open questions about how this lack of disclosure could affect a defendant's due process rights, such as whether some FRT results could constitute *Brady* evidence that must be disclosed to the defense.

With these costs in mind, it is easy to understand why many reasonable minds argue we simply must ban law enforcement use of FRT. I have wrestled with this conclusion myself. But ultimately, I still think it is possible to obtain the benefits of this technology while ensuring that we eliminate to the greatest degree possible the harms. And the way to do that is through sound and comprehensive regulation. This is not a revelatory concept – one need only look to the way Congress has approached the use of another invasive biometric in the criminal justice system—DNA—for regulatory inspiration.¹⁷ Of course there are substantive and procedural differences between these two biometrics and their use by law enforcement, but the caution with which Congress and other legislative bodies has approached DNA stands in stark contrast to what has happened with FRT. I cannot say this enough times: technologies like FRT simply should not be used without a regulatory framework in place that imposes strict controls around their use and ensures that they serve communities, particularly historically marginalized communities and specifically Black communities. Anything else is simply irresponsible.

¹⁵ Alex Holdor-Lee, *Privacy expert Clare Garvie explains why your face is already in a criminal lineup*, DOCUMENT JOURNAL (Oct. 12, 2020), <https://www.documentjournal.com/2020/10/privacy-expert-clare-garvie-explains-why-your-face-is-already-in-a-criminal-lineup/>.

¹⁶ Joanne Cavanaugh Simpson & Marc Freeman, *South Florida police quietly ran facial recognition scans to identify peaceful protestors. Is that legal?*, SOUTH FLORIDA SUNSENTINEL (June 26, 2021), <https://www.sun-sentinel.com/local/broward/fl-ne-facial-recognition-protests-20210626-7sl15uuaqfbeda32mdlv3xwxi-htmlstory.html>.

¹⁷ Emily J. Hanson, *The Use of DNA by the Criminal Justice System and the Federal Role: Background, Current Law, and Grants*, CONG. RESEARCH SERV. (Jan. 29, 2021), <https://fas.org/sgp/crs/misc/R41800.pdf>.

V. Regulatory role for Congress

I want to turn now to what are some of the essential aspects of an adequate regulatory regime. Over the past many months, I've made it a point to have conversations with a diverse set of stakeholders, including technology vendors, law enforcement, civil rights and racial justice advocates and privacy experts to discuss the issue of law enforcement use of FRT. I owe the insight I bring to you today to these conversations. And although people I speak with disagree vehemently about such fundamental matters as whether FRT should be used at all, I find remarkable agreement about what is *not* okay – about what shoddy practices around the use of FRT look like, and what must not be permitted. I also have learned of holes in our knowledge about FRT that need to be filled, and ideally before it is used at any greater scale. These are the matters regulation must address before we think of using FRT responsibly.

The points I am about to make are not comprehensive.¹⁸ The Policing Project hopes in the not-too-distant future to release a detailed enumeration of necessary provisions and steps to regulate FRT. But the points I make below show the level of nuance and attention I think is missing from the debate over FRT at present. And they reinforce the fact that many, many agencies are using FRT today in ways that are not coming close to meeting these most basic requirements.

A. Key considerations for regulation¹⁹

- Law enforcement use of FRT should be transparent and accountable – to the general public and criminal defendants alike

First and foremost, no government agency ever should be using biometric identification technologies such as face recognition, that were not appropriated for, and approved by, a democratically-responsible body. Unfortunately, too often, agencies acquire these technologies in other, less transparent and accountable ways.²⁰ All this does is breed mistrust of the agency and the technology. Nothing is lost by disclosure and democratic approval, and everything is gained.

Second, all agencies that use or access FRT should be required to draft and disclose use policies. Often the best way to maximize the benefits of a technology, while minimizing harms, is by setting clear rules on how the technology is used and disclosing the use policies to the public. Among other things, these policies should include provisions describing authorized uses and users, training requirements, privacy protections, internal oversight mechanisms, audit processes, and penalties for misuse. They should be attentive to the harms of the technology, especially privacy and racial harms. They also should identify which vendors and software programs are being used.

¹⁸ Many of these ideas originate from collaboration with my colleague, Prof. Andrew Ferguson, from whom I've learned a great deal. See Barry Friedman & Andrew Guthrie Ferguson, *Here's a Way Forward on Facial Recognition*, N.Y. TIMES (Oct. 31, 2019), <https://www.nytimes.com/2019/10/31/opinion/facial-recognition-regulation.html>; see also generally Ferguson, *supra* note 3 (providing an in-depth analysis of how the Fourth Amendment intersects – and doesn't – with law enforcement use of FRT and suggestions for a regulatory framework).

¹⁹ As I was putting the finishing touches on this written testimony, I discovered U.S. GAO's recent report on forensic technology, which includes a discussion of FRT use by law enforcement. U.S. Gen. Accounting Office, *GAO-21-435SP Forensic Technology* (July 6, 2021). From my brief review, it appears that many of their findings (e.g., lack of specialized training for human reviewers; algorithm versions tested by NIST are not necessarily the versions procured by agencies) and their policy recommendations (increased training, standards, and transparency) are in line with my own views as stated here.

²⁰ Matthew Guariglia & Dave Mass, *How Police Fund Surveillance Technology is Part of the Problem*, EFF (Sept. 23, 2020), <https://www.eff.org/deeplinks/2020/09/how-police-fund-surveillance-technology-part-problem>.

Third, we need careful data collection on, and disclosure of, FRT use. That is the only way we as a society will learn about best practices and the scope of any benefits. And such disclosure is of course essential to criminal defendants who are identified using FRT. For each use of FRT by law enforcement, the following information at a minimum should be collected and disclosed: which probe images are used and their quality, what matches were returned by the system, and investigative outcomes.

- Searches should not be limited to criminal databases

The choice of enrollment database—i.e., which repository of images that a probe image gets searched against—matters hugely when it comes to the impacts of law enforcement’s FRT use. Some agencies search only criminal (“mugshot”) databases; while others access statewide DMV databases. As I’ve written elsewhere, I believe that FRT should not be limited to criminal databases.²¹ This may sound counterintuitive, but these databases are the product of decades of discriminatory policing for offenses like drug crimes; using those will continue us on this course. And if the goal is to identify suspects, witnesses, and victims, then using a wider dataset only makes more sense. To yield more equitable and effective results, the police should search databases that include all our faces. If we permit the use of this technology, we should all be in the pool.

- Accuracy and fairness of the technology

Accuracy and bias are headline news when it comes to FRT. And you’ve likely heard claims about accuracy – such as vendors that tout near perfect accuracy in percentage terms, such as 90% accurate. But it is meaningless to talk about accuracy percentages. What matters with technologies like FRT is false positives (people identified as matches who are not) and false negatives (when there is a match in the database that is not returned). Every FRT system has to make tradeoffs between these; no system can get it exactly right. If we are looking for a lost child, we want fewer false negatives; if we are trying not to turn innocent people into suspects, we want fewer false positives. And how well FRT performs in terms of false positives and false negatives is a result of a number of factors that are not getting enough attention.

To effectively evaluate false positive and false negatives rates, we need independent testing of FRT systems under real world conditions, on the right size databases, and on the types of images law enforcement actually searches. This testing also needs to report error rates by demographic group and evaluate the impact of human review. None of this is happening today – at least not in any way that’s publicly reviewable.

The National Institute of Standards and Technology (NIST) currently runs the leading technical benchmark for FRT algorithms and its work in this area has been essential for improving the technology’s accuracy and providing public information about these algorithms. But NIST’s testing program, for all its value, tells us little about actual law enforcement use contexts:

- (1) NIST doesn’t test the algorithms that law enforcement actually uses. Rather, it tests whatever a vendor submits, which, depending on which vendor you ask, may be an algorithm that’s similar to what it sells to law enforcement, or it may not be at all.

²¹ Friedman & Ferguson, *supra* note 18.

- (2) NIST's testing databases are too small. *The literature makes clear that enrollment database size affects algorithmic accuracy and demographic bias.*²² As the Government Accountability Office's recent report revealed, NIST's largest testing database is way smaller than many law enforcement databases (in one case, 69 times smaller).²³ We can't know how well the technology performs in many law enforcement use contexts without evaluating them on larger databases.
- (3) NIST hasn't evaluated demographic performance on the types of images most commonly used by law enforcement, e.g., surveillance camera images. Making matters worse, these images typically are lower quality than images like mugshots and NIST's testing shows that error rates rise exponentially on lower quality photos. Without demographic breakdowns on operationally representative images, we have no idea how these algorithms perform for different subpopulations when deployed; and
- (4) Finally, NIST's testing program only evaluates algorithms; it doesn't evaluate the impact that human reviewers have on accuracy and bias. So its tests don't tell us anything about full system performance.

These deficiencies in NIST's testing are a huge problem because when it comes to publicly available independent, expert testing, NIST is the only game in town.

To solve this problem, Congress should give NIST the necessary resources to build a better technical benchmark, i.e., one that mirrors law enforcement use contexts. Congress also needs to invest in research for developing full-system operational testing that can evaluate both quantitative metrics (like error rates, broken out by demographics) and more qualitative metrics (like fairness and privacy).

- Human-in-the-loop

Evaluating and validating the tech itself is a necessary condition for regulating FRT, but it is not sufficient. We need to get the human part of this analysis right too.

You've probably heard the term "human-in-the-loop" offered up as a meaningful safeguard: we are told not to worry about FRT accuracy and bias, because in law enforcement situations a human checks the machine's outputs to confirm them. But once again, how this phrase is used is too simplistic and overlooks real issues. It ignores simple facts like that people tend to believe too deeply in, and be persuaded by, what technology tells them. In order to make the human-algorithm pairing work well, several things need to be done.

Human examiners should receive specialized training on both face comparison and the software.

Agencies should require that any officer who reviews FRT results is trained in the latest science on face comparison. Research has shown that forensically trained face examiners are better at recognizing faces than untrained individuals.²⁴ Although consensus standards for face

²² E.g., Li & Jain *supra* note 9 at 644.

²³ U.S. Gen. Accounting Office, GAO-21-518, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks* 16, Fig. 3 (2021).

²⁴ P. Jonathan Phillips et al., *Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms*, PNAS (2018), <https://www.pnas.org/content/115/24/6171>.

comparison still are under development, there are available resources that agencies can draw on today to train their officers.²⁵ In addition, examiners should receive vendor-supported training on the technical requirements and specifications of the software so they understand the ins-and-outs of how these systems function and how they can fail. This means explanations on things like how image quality and variations in an individual's appearance (glasses; bangs; hats) and other environmental factors can affect error rates. It also should include comprehensive training on the software's logging capabilities to ensure audit trails are created.

Research is needed to set standards on human-algorithm interaction.

We should treat face recognition like we do other forensics. For example, in criminal investigations, the best practice for witness identification of suspects is to “blind” the process. The law enforcement individual conducting a photo array does not know which of the photos is the suspect, and that way cannot unintentionally signal correct answers to the witness. We need to think about processes to “blind” the human in the loop so that in evaluating results from the algorithm, they are able to conduct an independent evaluation rather than over-trust the machine output.

Unfortunately, we don't know enough about the best practices in this area. Understanding how humans and machines work best together is an area of ongoing research. Some research shows that face recognition is most accurate when humans and machines work together.²⁶ On the other hand, automation bias (i.e., humans over-rely on machine output) is a well-studied phenomenon.²⁷ Congress should spearhead the development of consensus standards and best practices for the human component of FRT analysis and develop research-backed processes and protocols for conducting these examinations in ways that maximize accuracy and minimize bias.²⁸

In the meantime, however, there are some best practices we can implement right now: namely, agencies only should allow trained officers who are uninvolved in the underlying investigation to review FRT results. In addition, FRT results should be subject to multiple levels of independent human review before any action is taken, to reduce the impact of automation bias.

Develop a gold standard process for investigative corroboration.

While we're on the lookout for potentially meaningless terms, we also should view with skepticism any assurances that face recognition results are “not considered positive identifications” and that “further investigation is required.”²⁹ Just as there are no consensus

²⁵ See, e.g., *Facial Identification Subcommittee*, <https://www.nist.gov/osac/facial-identification-subcommittee> (listing proposed and passed standards for face comparison); *Facial Identification Scientific Working Group*, <https://www.fiswg.org/documents.html> (providing training, comparison and evaluation resources).

²⁶ Philips et al., *supra* note 21.

²⁷ Daniel E. Ho et al., *Evaluating Facial Recognition Technology: A Protocol for Performance Assessment in New Domains*, Stanford Instit. for Human-Centered AI 14 (Nov. 2020), https://hai.stanford.edu/sites/default/files/2020-11/HAI_FacialRecognitionWhitePaper.pdf; see also John J. Howard, et al., *Human-algorithm teaming in face recognition: How algorithm outcomes cognitively bias human decision-making*, PLOS ONE (2020), <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0237855>.

²⁸ I acknowledge that some of this work is underway, see, e.g., entities like OSAC's Facial Identification Subcommittee. E.g., *Facial Identification Subcommittee*, <https://www.nist.gov/osac/facial-identification-subcommittee>. My remarks here are directed at emphasizing the need to support—not supplant—this type of work.

²⁹ E.g., Det. Police Dep't, *Directive No. 307.5 Facial Recognition* § 307.5-5.4, <https://detroitmi.gov/sites/detroitmi.localhost/files/2019->

standards for human review of FRT results, there is no common best practice for what constitutes sufficient investigative follow up to confirm an FRT lead. I have no doubt that many agencies and individual officers take this requirement to heart and engage in thorough, independent investigative efforts after receiving an FRT lead. Still, Mr. Robert Williams' story, whose testimony you also will hear today, provides a painfully real reminder that others do not.

Federal agencies like the Federal Bureau of Investigation and the Department of Homeland Security are avid users of this technology for investigative identifications and likely have significant expertise in this area. There is both an opportunity and a need for federal agencies, in conjunction with defense and civil rights and racial justice experts, to develop gold standard processes for the investigative follow up that should be required to corroborate an FRT lead that then could serve as a model for local agencies.

- Law enforcement use of FRT for face identification should be limited and legitimate

Considering the various and serious harms that can result from law enforcement use of FRT, agencies need to have good reason to deploy this tool. To my mind, using FRT to investigate serious crimes, like murder, rape and child kidnapping, is a good reason. Using FRT to investigate petty crime or to search for unlawful immigrants, is not. Overcriminalization is an epidemic in our country and one that disproportionately affects people of color, particularly in Black and brown communities. Unless we limit face identification to serious offenses, we will exacerbate this problem.

We also need to have proof of officers' "predicate" for using the technology at all. In the past, I have advocated for a warrant requirement to ensure face identification is used only as permitted. I still believe this approach makes sense - without a requirement for neutral supervision, there simply is too much potential for abuse. (This belief also is reflected in Maine's recent bipartisan legislation regulating law enforcement use of FRT – one of the few states that has managed to take action on this issue). Before FRT is used, a judge should be persuaded that the probe photo represents a real suspect for an enumerated offense.

- Regulate Vendors

Congress unquestionably has power to regulate the vendors of FRT products and it should. The vendors of high-risk technology products like FRT bear responsibility for ensuring their products work as promised and do not perpetuate harmful bias. Regulators in Europe have recognized this; the European Commission's recent regulatory framework proposal on AI sets forth a series of pre-market conformity requirements that vendors must meet before they can sell "high-risk" AI systems.³⁰ In a similar vein, NIST recently issued a draft report on managing AI bias that includes a detailed set of recommendations directly targeting AI developers. Vendors have a role to play in ensuring the ethical operation of their systems – and Congress should require that they do so.

[09/Revised%20facial%20recognition%20directive%20transmitted%20to%20Board%202019-12-2019.pdf](#); *NYPD Questions and Answers Facial Recognition*, <https://www1.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page>.

³⁰ *Regulatory framework proposal on Artificial Intelligence, European Commission*, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.

To give some examples, Congress should require that vendors:

- ⇒ Train their algorithms on datasets that are designed to mitigate harmful bias. This means building datasets that are sufficiently diverse and representative of the population in which it will be deployed and that don't perpetuate historical biases.
 - ⇒ Consider factors other than raw accuracy when selecting which models to develop – in particular, vendors should have to consider accuracy for the relevant subpopulations that stand to be impacted by their technology.
 - ⇒ Ensure their FRT products are self-auditing, i.e., that they are built with sufficient capabilities to log user actions and trace results, so that law enforcement agencies can audit themselves and make public disclosure.
 - ⇒ Provide documentation of all internal testing and error rate reporting for their systems.
 - ⇒ Provide comprehensive user training on the technical requirements and specifications of their products.
 - ⇒ Set criteria around things like image quality specifications required to ensure system accuracy and ensure that users cannot submit or modify images that don't meet these specifications.
- Facilitate fact-finding to guide development of best practices

Finally, as I noted above, the discourse around the benefits and harms of FRT suffers from a massive information gap. We don't know how many agencies are using this technology; we don't know how many cases it helped solve; or how often its use has led to misidentifications. Congress can help fill these knowledge gaps by providing federal funding for the local data gathering that is necessary to evaluate the use and impact of this tool.

Conclusion

As I said, this is not a complete list. But I hope I have convinced you of two things:

First, there is a crying need for regulation of FRT technology, now. No matter where you are on the pro-con debate over FRT, you must recognize—as so many with whom I have spoken do—that permitting its use without regulation of some of these key elements is risky, unacceptable, certain to lead to racial bias, and undemocratic.

Second, the proper use of FRT is a complicated matter, and it requires regulation that matches that complexity.

I want to thank you for the opportunity to testify today. The matter you are considering is extremely consequential. We all should want optimal outcomes and rational solutions.

We would of course be willing to provide any other information that could be of use.

Ms. JACKSON LEE. Thank you very much, Professor Friedman.

It's now my pleasure to recognize Mr. Robert Williams.

Welcome, Mr. Williams. Again, I indicated my apologies. We are the presiders over law enforcement in this Nation, and, certainly, we welcome your very important testimony. Thank you.

You are recognized for five minutes.

STATEMENT OF ROBERT WILLIAMS

Mr. WILLIAMS. Thank you. Okay. Chair Nadler, Chair Jackson Lee, Ranking Member Jordan, Ranking Member Biggs, and Members of the Subcommittee, thank you for the opportunity to testify today.

Last—well, not last, but January 2020, I got a call from my wife, and she told me that some detectives called her to tell me to turn myself in. She said they'd be calling me shortly because they didn't have my phone number.

They called me. I answered and said—I asked them what it was about. He told me he couldn't tell me. All we know is that I need to turn myself in.

I assumed it was a prank call, and I hung up and called my wife and told my wife to disregard it, who was irate and thinking that maybe I was trying to hide something from her.

So, I told her to call our local police department. She did. They said they had no warrants or anything for my arrest and I should disregard the call.

So, I proceeded to drive home. When I got home, there was a Detroit police car parked on my street. When I pulled in the driveway, he pulled in my driveway and blocked me in as if I was going to make a run for it.

He pulled up. He said, "Are you Robert Williams?" I said, "Yes, I am." He said, "You're under arrest." I said, "Whoa, you can't just arrest me for that. What am I under arrest for?" He said, "Don't worry about it," and proceeded to put the handcuffs on me.

I told my wife and my kids who were coming out of the house at the time, "Don't worry about it, they are making a mistake. I'll be right back."

Unfortunately, I wasn't right back. I ended up spending 30 hours in jail—well, at the detention center.

While I was in the car, I asked them again, "Why am I being arrested?" They said, "We can't tell you that." They showed me the warrant that said "felony larceny" on it. I'm like, "I didn't steal anything." I'm like, "How do we get the warrant?" He said that a detective will be in to talk to me.

I was in the detention center in an overcrowded cell. The garbage was overflowing. There was a lot of less desirables in there talking about things that they had done and things that they had got away with. I am just like, "Why am I here?" Nobody ever came to tell me.

So, the next day, when I went to court, I pleaded not guilty. They took a recess, and then some detectives came and asked me some questions. When they came to ask questions, they had me sign a paper saying that I will waive my right to counsel so they could show me what was on the papers. I signed.

He showed me a picture. He said, "When was the last time you was at the Shinola store?" I said, "A couple of years ago." He said, "So, that's not you?" I said, "No, that's not me."

He turns over another piece of paper. He said, "So, I guess that's not you either?" I held that piece paper up to my face and said, "I hope you don't think all Black people look alike."

He turned over another paper and said, "So, I guess the computer got it wrong." I am like, "I guess so. Am I free to go?" He was like, "I'm sorry for this mishandling, but we're not the detectives on your case so we can't let you go," so they sent me back to my cell.

I got out. I received a bond, and I got out. My wife contacted the ACLU, and we started getting the information about the case, and we realized that it was a wrong facial recognition technology used.

I just have been fighting for it ever since. I just don't think it's right that my picture was used in some type of lineup, and I have never been in trouble.

With that being said, I would just like to say thank you for the opportunity to share my testimony. I hope that Congress does something about this law. I am happy to take any more questions that you might have for me.

[The statement of Mr. Williams follows:]

Testimony of Robert Williams

House of Representatives
Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security

Hearing On

“FACIAL RECOGNITION TECHNOLOGY: EXAMINING ITS USE BY LAW
ENFORCEMENT”

July 13, 2021

Chair Nadler, Chair Jackson Lee, Ranking Member Jordan, Ranking Member Biggs, and members of the Subcommittee, thank you for the opportunity to testify today about the dangers of law enforcement uses of facial recognition technology.

I never thought I would be a cautionary tale. More than that, I never thought I'd have to explain to my daughters why their Daddy got arrested in front of them on our front lawn. How does one explain to two little girls that a computer got it wrong, but the police listened to it anyway and that meant they could arrest me for a crime I didn't commit?

This is what happened to me: As I was getting ready to head home from work one day in January of 2020, my wife called me and told me that a police officer had called and said I needed to turn myself in. She was scared and confused. The officers called me next, but wouldn't explain why I was supposed to turn myself in or what I was accused of, so I thought it was probably a prank. I couldn't imagine what else it could be. But as I pulled up to my house, a Detroit police squad car was waiting for me. When I pulled into the driveway, the squad car swooped in from behind to block my SUV — as if I would make a run for it. One officer jumped out and asked if I was Robert Williams. I said I was. He told me I was under arrest.

I asked for a reason. He showed me a piece of paper with my name on it. The words "arrest warrant" and "felony larceny" were all I could make out.

By then, my wife, Melissa, was outside with our youngest in her arms, and my older daughter was peeking around my wife trying to see what was happening. I told my older daughter to go back inside, that the cops were making a mistake and that Daddy would be back in a minute.

But I wasn't back in a minute. I was handcuffed and taken to the Detroit Detention Center.

As any other person would be, I was confused, scared, and, yes, angry, that this was happening to me. As any other black man would be, I had to consider what could happen if I asked too many questions or displayed my anger openly — even though I knew I had done nothing wrong.

When we arrived at the detention center, I was patted down probably seven times, asked to remove the strings from my shoes and hoodie and fingerprinted. They also took my mugshot and DNA sample. No one would tell me what crime they thought I'd committed.

After that, a full 18 hours went by. I spent the night sleeping on the cold concrete floor of a filthy, overcrowded cell next to an overflowing trash can. No one came to talk to me or explain what I was accused of.

Meanwhile, my family spent the night at home, without me, scared for me and for what my false arrest would mean for all of us.

Finally, the next morning, two officers came to talk to me. They refused to explain what I was accused of unless I waived me right to have an attorney present, so that's what I did because I was so desperate to learn why I was being incarcerated. They asked if I'd ever been to a Shinola watch store in Detroit. I was honest. I said that I had been to one once, many years ago. They showed me a blurry surveillance camera photo of a black man and asked if it was me. I chuckled a bit. "No, that is not me." One of the officers showed me another photo and said, "So I guess this isn't you either?" It wasn't. I picked up the piece of paper, put it next to my face and said, "I hope you guys don't think that all black men look alike."

The cops looked at each other. I heard one say that "the computer must have gotten it wrong." I asked if I was free to go now, and they said no. I returned to my cell to await what would come next. I was released from detention later that evening, after nearly 30 hours in holding.

They released me into a cold, rainy night in Detroit. I had to wait on the corner for 45 minutes for my wife to be able to come pick me up, which was not easy for her to do since we have two young children and it was after their bedtime.

I should also mention that during the time that I was in custody, my wife was dealing with the emotional and practical immediate fall out. My daughters were scared, wondering why their father had been arrested and whether he would come home. My wife had to comfort them. While I was away, our oldest daughter turned over a family photo that was sitting out on the family furniture because she couldn't bear looking at a picture of her Daddy under the circumstances. My wife also had to call my employer and explain to them where I was and why I wouldn't be coming to work that day. They could have fired me right then. They didn't and for that I'm grateful. But they could have. I hate to think of what could have happened to my family if they had.

I eventually got more information after the American Civil Liberties Union of Michigan connected me with a defense attorney. Someone had stolen watches, and the store owner provided surveillance footage to the Detroit Police Department. They sent a blurry, shadowy image from that footage to the Michigan State Police, who then ran it through their facial-recognition system. That system incorrectly matched a photograph of me pulled from an old driver's license picture with the surveillance image.

I've since learned that federal studies [have shown](#) that facial-recognition systems misidentify Asian and Black people up to 100 times more often than white people. Why is law enforcement even allowed to use such technology when it obviously doesn't work? I get angry when I hear companies, politicians and police talk about how this technology isn't dangerous or flawed or say that they only use it as an investigative tool. If any of that was true, I wouldn't have been arrested.

What's worse is that, before this happened to me, I actually believed them. I thought, "what's so terrible if they're not invading our privacy and all they're doing is using this technology to narrow in on a group of suspects?"

We now know that there are at least two others like me who were arrested for crimes they didn't commit because the computer made a mistake – both Black men. According to the Georgetown Privacy Law Center, there are undoubtedly many more. The only question is how many because police and prosecutors often do not think that they are obligated to disclose when they use facial recognition to identify people. I wouldn't have known that facial recognition was used to arrest me had it not been for the cops who let it slip while interrogating me. In that way, I got lucky, if you can call it that. Others, we can be sure, were not.

Lawyers at the ACLU and the University of Michigan's Civil Rights Litigation Initiative have filed a lawsuit against the police department on my behalf, but winning that case can't undo the damage to me and my family. My daughters can't unsee me being handcuffed and put into a police car. They continue to suffer that trauma. For example, after I returned from Jail, they started playing cops and robbers games where they tell me that I'm in jail for stealing. And even today, when my daughters encounter the coverage about what happened to me, they are reduced to tears by their memory of those awful days. We just don't know what kind of long-term impact this might have on them; we do know that this was their first ever encounter with the police.

But they can also see me use this experience to bring some good into the world. That means helping make sure my daughters don't grow up in a world where their driver's license or Facebook photos could be used to target, track or harm them – or anyone else. That's why I brought the case with the ACLU and it's why I'm here talking to you today.

I also want to say something about improving the accuracy of the technology. I don't want anyone to walk away from my testimony thinking that if only the technology was made more accurate, its problems would be solved. Even if this technology does become accurate (at the expense of people like me), I don't want my daughters' faces to be part of some government database. I don't want cops showing up at their door because they were recorded at a protest the government didn't like. I don't want this technology automating and worsening the racist policies they could be protesting. I don't want them to have a police record for something they didn't do — like I now do.

I grew up in Detroit, and I know from that experience that the fact of the matter is that people that look like me have been long been more subject to surveillance, heavy policing, and mass incarceration than other some other populations. I worry that facial recognition technology, even if it works better than it did in my case, will make these problems worse.

That's why I think Congress should stop law enforcement from using facial recognition technology. As it is, it's just too dangerous. There's legislation that could help get the job done. The Facial Recognition and Biometric Technology Moratorium Act would stop

federal law enforcement using this technology and make it harder for state and local cops to pay for it too.

I keep thinking about how lucky I was to have spent only one night in jail — as traumatizing as it was. Many Black people won't be so lucky. My family and I don't want to live with that fear. I don't want anyone to live with that fear. Congress should do something to make sure no one else has to. I truly hope that you will.

Thank you again for the opportunity to testify today. I am happy to answer any questions.

Ms. JACKSON LEE. Powerful statement, Mr. Williams. You are tracking what I began with as I opened this hearing, that not only should we engage in oversight, but I do think we should engage in the right kind of fix. I am very apologetic to you and your family for having to go through this.

Our next Witness is Mr. Bertram Lee, Jr. You are recognized for five minutes.

STATEMENT OF BERTRAM LEE, JR.

Mr. LEE. Chair Jackson Lee, Chair Nadler, Ranking Member Jordan, Ranking Member Biggs, and Members of the Subcommittee, thank you for the opportunity to testify today.

Thank you, Chair Jackson Lee and Chair Nadler, for calling this hearing and shining a light on the serious and undeniable threat that facial recognition technology poses, especially to Black and Brown people and other marginalized communities.

We are at a turning point. We must reject policies and practices rooted in discrimination towards marginalized communities and move toward a new paradigm for public safety that respects the humanity, dignity, and human rights of all people.

The Leadership Conference has spoken out against law enforcement use of facial recognition since 2016, how we're adding the inherent bias of these tools and their disparate impact on marginalized communities that are already overpoliced.

Last month, The Leadership Conference, along with Upturn and New America's Open Technology Institute, released a statement signed by 40 advocacy organizations that outlined six of our most pressing civil rights concerns about facial recognition technology, including that its use exacerbates the harms of policing in communities that are already targeted by police; threatens individual and community privacy by allowing invasive and persistent tracking and targeting; chills First Amendment-protected activities; violates due process rights and otherwise infringes upon procedural justice; often relies on face prints that have been obtained without consent.

Lastly, in addition to racial bias with respect to how law enforcement uses facial recognition, the technology itself poses a disproportionate risk of misidentification for Black, Asian, and Indigenous people.

The possibility for misidentification and misclassification poses a tremendous threat to the health, safety, and well-being of communities. The reason for these problems and inherent biases varies. In some cases, the cause of the bias lives within the database that an image is searched against. In others, it is due to the historical bias built into the algorithm itself.

The end result, however, is the same: Black people are disproportionately represented in law enforcement facial recognition databases, and inequitable error rates further entrench racial disparities in the criminal legal system.

For example, in a comparison of match rates by country of origin, photos of people from East African countries had false rates a hundred times higher than the baseline rate. Researchers also found that some facial analysis algorithms misclassified Black women nearly 35 percent of the time while always getting it right for White men.

Even if the accuracy of facial recognition technology was improved, the fundamental issue remains: Facial recognition technology dangerously expands the scope and power of law enforcement.

When combined with existing networks of surveillance cameras dotting our urban and suburban landscapes, facial recognition algorithms could enable governments to track the public movements, habits, and associations of all people at all times, merely with the push of a button.

According to a report from the Georgetown Center on Privacy and Technology, more than 133 million American adults are included in facial recognition networks across the country, and at least one in four State or local police departments can run facial recognition searches through their own network or the network of another agency.

As facial recognition technology rapidly emerges in everyday police activities, safeguards to ensure this technology is used fairly and responsibly are virtually nonexistent.

As Congress considers how our Nation's systems of policing and punishment disproportionately harm communities of color, it must decelerate law enforcement's ability to wield such powerful technology, particularly when the history and recent abuses provide little reason to think it would be used responsibly.

We are safer when our communities are healthy, well-resourced, and thriving. Policies of mass criminalization and over policing are fueled by White supremacy, not a belief in justice, and tools like facial recognition technology are about social control, not public safety.

The Leadership Conference urges Members of Congress to Act now to protect the public from this technology, specifically by implementing a ban or moratorium on law enforcement use of facial recognition tools.

Families and communities will continue to endure unspeakable harm and tragedy on our government's watch as long as we allow these policies to continue. Time is of the essence.

The Leadership Conference looks forward to working closely with the Subcommittee to address the serious concerns with this technology and work toward a new vision of justice that truly keeps communities safe.

Thank you.

[The statement of Mr. Lee follows:]

The Leadership Conference
on Civil and Human Rights

1620 L Street, NW
Suite 1100
Washington, DC
20036
202.466.3311 voice
202.466.3435 fax
www.civilrights.org



**STATEMENT OF BERTRAM LEE, COUNSEL FOR MEDIA AND TECHNOLOGY
THE LEADERSHIP CONFERENCE ON CIVIL AND HUMAN RIGHTS**

**U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY**

**HEARING ON “FACIAL RECOGNITION TECHNOLOGY: EXAMINING ITS USE
BY LAW ENFORCEMENT”**

JULY 13, 2021

Chairwoman Jackson-Lee, Chairman Nadler, Ranking Member Jordan, Ranking Member Biggs, and members of the subcommittee: My name is Bertram Lee, and I am Counsel for Media and Technology at The Leadership Conference on Civil and Human Rights, a coalition charged by its diverse membership of more than 220 national organizations to promote and protect the civil and human rights of all persons in the United States. Thank you for the opportunity to testify about the use of facial recognition technology by law enforcement.

Founded in 1950 by A. Philip Randolph, Arnold Aronson, and Roy Wilkins, The Leadership Conference works in support of policies that further the goal of equality under the law through legislative advocacy and public education. The Leadership Conference provides a powerful unified voice for the many constituencies of our coalition: persons of color, women, children, people with disabilities, LGBTQ people, older Americans, working people, immigrants, people of faith, civil libertarians, and human rights advocates. Given the breadth of our coalition, The Leadership Conference is uniquely positioned to address many of the most pressing issues affecting the nation today, including the need to transform the criminal-legal system in America and ensure that technology is designed and used in ways that respect civil rights.

The American criminal-legal system was built on a structure designed to capture humans escaping bondage, relying on community surveillance to not only capture, but also punish those seeking freedom.¹ Facial recognition technology, and the biases these systems contain, only serve to continue this history of discrimination and the disparate treatment of people of color in a new era. The expansion of surveillance technologies like facial recognition does not make communities of color safer; instead, it does the

¹ Connie Hassett-Walker, *The racist roots of American policing: From slave patrols to traffic stops*, The Chicago Reporter (June 7, 2019), <https://www.chicagoreporter.com/the-racist-roots-of-american-policing-from-slave-patrols-to-traffic-stops/>.



opposite.² Use of facial recognition in law enforcement only further exposes people of color to the systemic racism of the criminal-legal system, reinforcing racist narratives that Black communities and other people of color are to be surveilled and over-policed at every turn. That is why this hearing is so important, and we commend the subcommittee for much-needed and welcome attention on problematic uses of technology within our policing and criminal-legal system.

The Leadership Conference has spoken out against law enforcement use of facial recognition since 2016, highlighting the inherent bias of these tools and their disparate impact on marginalized communities that were already over-policed.³ Last month, The Leadership Conference, along with Upturn and New America's Open Technology Institute, released "Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology," which was signed by 40 advocacy organizations.⁴ The statement, which we request be entered into the record of this hearing, highlighted six of the most pressing civil rights concerns that advocacy organizations have with facial recognition technology:

1. Regardless of technical accuracy, law enforcement use of face recognition systems could exacerbate the harms of policing in communities that are already targeted by the police.
2. Law enforcement use of face recognition threatens individual and community privacy by allowing invasive and persistent tracking and targeting.
3. Law enforcement use of face recognition can chill First Amendment-protected activities.
4. Law enforcement use of face recognition can easily violate due process rights and otherwise infringe upon procedural justice.
5. Face recognition systems used by law enforcement often rely on faceprints that have been obtained without consent.
6. In addition to racial bias in how law enforcement use face recognition, the technology itself poses disproportionate risks of misidentification for Black, Asian, and Indigenous people.

² Frances Adams-O'Brien, *Is There Empirical Evidence That Surveillance Cameras Reduce Crime?*, Municipal Technical Advisory Service Institute for Public Service (September 26, 2016), <https://www.mtas.tennessee.edu/knowledgebase/there-empirical-evidence-surveillance-cameras-reduce-crime>.

³ The Leadership Conference on Civil and Human Rights, *Letter to Principal Deputy Assistant Attorney General Vanita Gupta* (October 18, 2016), https://www.aclu.org/sites/default/files/field_document/coalition_letter_to_doj_crt_re_face_recognition_10-18-2016_1.pdf; The Leadership Conference on Civil and Human Rights, *Letter to Committee on Oversight and Reform about Protests* (June 30, 2020), <https://civilrights.org/resource/letter-to-committee-on-oversight-and-reform-about-protests/>; The Leadership Conference on Civil and Human Rights, *Comments in Opposition to Proposed Rulemaking: Collection of Biometric Data from Aliens upon Entry to and Departure from the United States* (December 21, 2020), <https://civilrights.org/resource/comments-in-opposition-to-proposed-rulemaking-collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states/>; The Leadership Conference on Civil and Human Rights, *Civil Rights Groups Urge Strong Ethical Review of Axon's Police Technology* (April 26, 2018), <https://civilrights.org/2018/04/26/civil-rights-groups-urge-strong-ethical-review-axons-police-technology/>.

⁴ The Leadership Conference on Civil and Human Rights et al., *Civil Rights Concerns Regarding the Law Enforcement Use of Facial Recognition Technology* (June 3, 2021), https://newamericadotorg.s3.amazonaws.com/documents/FINAL_Civil_Rights_Statement_of_Concerns_LE_Use_of_FRT_June_2021.pdf.



Additionally, The Leadership Conference, the ACLU, and more than 45 advocacy organizations wrote a letter to the Biden administration calling for a moratorium on the government use of facial recognition technology.⁵

We urge policymakers to act now to protect the public from face recognition technology. The most effective way to do that is by implementing a ban or moratorium on law enforcement use of face recognition.

Facial Recognition Technologies Are Inherently Biased

Facial recognition technology disproportionately misidentifies and misclassifies people of color, trans people,⁶ women, and other marginalized groups, posing threats to communities' health, safety, and well-being. The reasons for these biases vary: In some cases, the cause of bias is the database an image is being searched against. In others, it is due to historical bias that is built into the algorithm through the images used to develop the technology. Some experts have even blamed inconsistent lighting. The end result, however, is the same: As the Center for Strategic and International Studies highlighted, "[e]ven if an algorithm shows no difference in its accuracy between demographics, its use could still result in a disparate impact if certain groups are over-represented in databases. African-American males, for example, are disproportionately represented in the mugshot databases many law enforcement facial recognition systems use for matching."⁷ In at least three cases that are publicly known, police have relied on erroneous face recognition identifications to make wrongful arrests of Black men. Robert Williams, who is also testifying before the subcommittee today, was one such individual and he will speak directly to the dangerous nature of this technology in the hands of law enforcement.

Studies of face recognition algorithms have found that commercial algorithms available for purchase and use by government entities around the country have inequitable error rates across a number of demographics, including race, sex, and age. The National Institute of Standards and Technology's Face Recognition Vendor Test found significant variation in both false positives (instances where the algorithm said there was a match when no such match existed), and false negative error rates (instances where the algorithm said there was not a match but there was one), across race, sex, and age. The highest false positives for U.S. law enforcement mugshots were among Black, Asian, and Indigenous people.⁸ In a comparison of match rates by country of origin, photos of people from East African countries had false

⁵ American Civil Liberties Union, *Facial Recognition Technology Letter to President Biden*, February 26, 2021, https://www.aclu.org/sites/default/files/field_document/02.16.2021_coalition_letter_requesting_federal_moratorium_on_facial_recognition.pdf.

⁶ Amrita Khalid, *Facial recognition AI can't identify trans and non-binary people*, Quartz (October 26, 2019), <https://qz.com/1726806/facial-recognition-ai-from-amazon-microsoft-and-ibm-misidentifies-trans-and-non-binary-people/>.

⁷ William Crumpler, *The Problem of Bias in Facial Recognition*, The Center for Strategic & International Studies (May 1, 2020), <https://www.csis.org/blogs/technology-policy-blog/problem-bias-facial-recognition>.

⁸ Patrick Grother, Mei Ngan, and Kayee Hanaoka, *NISTIR 8280: Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, National Institute of Standards and Technology (December 2019), <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>.



positive rates 100 times higher than the baseline rate.⁹

These findings are consistent with previous research conducted by Black scholars Joy Buolamwini, Deb Raji, and Timnit Gebru that concludes that algorithms could be racist. Their research found that some facial analysis algorithms misclassified Black women nearly 35 percent of the time, while nearly always getting it right for White men.¹⁰ A subsequent study by Buolamwini and Raji at the Massachusetts Institute of Technology confirmed these problems persisted with Amazon's facial recognition technology.¹¹

Bias in facial recognition technology is hardly surprising given that the technology, data, and history of the tools, standards, and practices are based in racist systems. Cameras at their inception were not meant to portray the faces of Black and Brown people the same way they portrayed White people.¹² These tools were not designed with people of color in mind, calling into question whether we can reasonably rely on a camera to tell us the "truth."

Yet rather than investigating these tools and practices, law enforcement instead tests them on the bodies of people of color, further exacerbating the harms created by the criminal-legal system itself. Some families never recover, financially or psychologically, from a close relative's encounter with the criminal-legal system.¹³ By continuing to use facial recognition technologies that are deeply biased against the very same communities that are targeted by surveillance and policing, law enforcement threatens to further entrench the current criminal-legal apartheid system of justice.

Improving Accuracy Will Not Mitigate the Disparate Impact of Facial Recognition

Improvements in the accuracy of facial recognition technology will not address the fundamental issue that facial recognition technology expands the scope and power of law enforcement, an institution that has a long and documented history of racial discrimination and racial violence that continues to this day. In the context of policing, facial recognition is always dangerous — no matter its accuracy. Throughout our nation's history, law enforcement has used surveillance to silence dissent and to maintain white supremacy, as evidenced from slave patrols to the FBI's COINTELPRO program.¹⁴ Facial recognition and other modern surveillance technologies promise to continue a history that has shown itself to be

⁹ *Id.*

¹⁰ Joy Buolamwini, Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91, 2018, <http://proceedings.mlr.press/v81/buolamwini18a.html>.

¹¹ Natasha Singer, *Amazon Is Pushing Facial Technology That a Study Says Could Be Biased*, The New York Times (January 24, 2019), <https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html>.

¹² Sarah Lewis, *The Racial Bias Built Into Photography*, The New York Times (April 25, 2019), <https://www.nytimes.com/2019/04/25/lens/sarah-lewis-racial-bias-photography.html>.

¹³ *Incarceration's Impact on Kids and Families*, The Vera Institute for Justice (2016), <http://humantolofjail.vera.org/the-family-jail-cycle/>.

¹⁴ Devlin Barrett, *FBI pressured to answer for domestic-spying program tied to Black Panther Fred Hampton's killing in 1969*, The Washington Post (May 4, 2021), <https://wapo.st/3hN2HTD>.



incompatible with the freedoms and rights of Black and Brown communities.

Even if the technology worked perfectly, it would still facilitate the mass tracking of people's movements in public spaces, a point highlighted in the recent revelation that the Los Angeles Police Department was spying on Black Lives Matter protestors using Amazon Ring cameras.¹⁵ When combined with existing networks of surveillance cameras dotting our urban and suburban landscapes, facial recognition algorithms could enable governments to track the public movements, habits, and associations of all people, at all times — merely with the push of a button. In the year 2021, the persistent tracking of all people in America's public spaces with facial recognition technology is no longer relegated to the realm of science fiction; it is now our reality. As Congress considers how our nation's systems of policing and justice disproportionately harm communities of color, it must decelerate law enforcement's ability to wield such a powerful technology when history and recent abuses provide little reason to think it will be used responsibly.

Facial Recognition Technologies Only Expand the Current Police State

In a disturbing development, federal, state, and local law enforcement are increasingly using facial recognition technology for routine investigations, and facial recognition networks have grown to include half of all American adults. According to a report from the Georgetown Center on Privacy and Technology, more than 133 million American adults are included in facial recognition networks across the country, and at least one in four state or local police departments can run facial recognition searches through their own network or the network of another agency.¹⁶ For example, the Sheriff's Office in Pinellas County, Florida, alone estimates that more than 8,000 facial recognition searches are conducted on its system every month.¹⁷ Similarly, the FBI is expanding the reach of its face recognition unit (FACE Services), through which it can access more than 30 million photos in its own database and scan the driver's license photos of 16 states.¹⁸ From August 2011 through December 2015, the FBI requested nearly 215,000 searches of external partners' databases alone. Last Congress, the FBI confirmed that it has the ability to match against more than 640 million photos.¹⁹

¹⁵ Matthew Guariglia and David Maass, LAPD Requested Ring Footage of Black Lives Matter Protests, Electronic Frontier Foundation (February 26, 2021), <https://www.eff.org/deeplinks/2021/02/lapd-requested-ring-footage-black-lives-matter-protests>.

¹⁶ Facial Recognition Technology (Part 1): Its Impact on Our Civil Rights and Liberties, U.S. House of Representatives Committee on Oversight and Reform, 115th Congress (2019), Statement of Clare Garvie, Senior Associate, Center on Privacy & Technology at Georgetown Law, <https://www.congress.gov/116/meeting/house/109521/witnesses/HHRG-116-GO00-Wstate-GarvieC-20190522.pdf>; Clare Garvie, Alvaro M. Bedoya, & Jonathan Frankle, The Perpetual Line-Up: Unregulated Police Face Recognition in America, Center on Privacy & Technology at Georgetown Law (Oct. 18, 2016) <http://www.perpetuallineup.org>.

¹⁷ Jerry Iannelli, Miami-Dade Cops Want Permanent Access to Controversial Facial Recognition Database, Miami New Times (November 8, 2019), <https://www.miaminewtimes.com/news/miami-dade-police-department-wants-to-use-pinellas-county-faces-facial-recognition-database-11313634>.

¹⁸ Government Accountability Office, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy* (May 2016), <http://www.gao.gov/assets/680/677098.pdf>.

¹⁹ Russell Brandom, *Facebook, Twitter, and Instagram Surveillance Tool Was Used to Arrest Baltimore Protestors*, The Verge (October 11, 2016), <http://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police->



Though facial recognition technology is rapidly merging with everyday police activities in nearly every jurisdiction in America,²⁰ the safeguards to ensure this technology is being used fairly and responsibly are virtually nonexistent. The FBI and other federal law enforcement agencies have been using facial recognition technology for years and without explicit authorization or guidance from Congress. That must be corrected, but law enforcement use is not the only concern. Facial recognition technology is being deployed in schools, workplaces, public housing developments, and health care facilities, in many cases to devastating effect.²¹

For instance, in schools, Black and Brown children are disproportionately disciplined compared to their White counterparts for the same behavior.²² Introducing facial recognition technology into an already discriminatory environment compounds the negative and disparate impacts on Black and Brown children by increasing their interactions with school officials and greasing the school-to-prison pipeline. There is already evidence that law enforcement is using facial recognition technology not only on major cases but minor ones as well.²³ The use of facial recognition in minor or misdemeanor investigations only adds to the disparate policing that people of color and LGBTQ people experience on a daily basis. LGBTQ youth are particularly targeted by law enforcement and incarcerated at much higher rates compared to heterosexual/cisgender youth.²⁴

Law enforcement is expanding its surveillance powers at a time when many Americans are becoming increasingly cognizant of police abuses, as evidenced by the nationwide protests for police accountability over the past year. If the government can track everyone who goes to a place of worship, attends a political rally, or seeks health care for reproductive health or substance use, we lose our freedom to pray to the god we want, speak our minds, freely criticize the government, and access health care in private. Americans should feel free to do these things without fear that government officials are secretly tracking and cataloging their every move.

Over the past two years, activists have pushed local leaders to pass bans on government use of facial

surveillance-geofeedia-api.; Neema Singh Guliani, *The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database*, American Civil Liberties Union (June 7, 2019), <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-p-photos-through>.

²⁰ Supra note 13.

²¹ Alfred Ng, *This Manual for a Popular Facial Recognition Tool Shows Just How Much the Software Tracks People*, The Markup (July 6, 2021), <https://themarkup.org/privacy/2021/07/06/this-manual-for-a-popular-facial-recognition-tool-shows-just-how-much-the-software-tracks-people>.

²² Brett Arends, *Black children are more likely to be disciplined than white kids for the same behavior*, Marketwatch (October 16, 2019), <https://www.marketwatch.com/story/black-children-are-more-likely-to-be-disciplined-than-white-kids-for-the-same-behavior-2019-10-16>.

²³ Alfred Ng, *Police are using facial recognition for minor crimes because they can*, CNET (October 24, 2021), <https://www.cnet.com/tech/services-and-software/police-are-using-facial-recognition-for-minor-crimes-because-they-can/>.

²⁴ See, e.g., Movement Advancement Project et al., *Unjust: LGBTQ Youth Incarcerated in the Juvenile Justice System* (June 2017), <https://www.lgbtmap.org/criminal-justice-youth-detention>.



recognition in at least 20 municipalities across the country, including Boston, Mass., San Francisco, Calif., and Jackson, Miss.²⁵ States including Vermont, California, Maine, Virginia, and New York have passed legislation halting some government use of the technology, particularly in light of the substantial racial justice and constitutional concerns detailed above. Unfortunately, however, local and state governments are largely powerless to control the way the FBI and other federal agencies use this technology in communities. As more jurisdictions place a moratorium on facial recognition technology, Congress needs to have a larger conversation about not only federal use of facial recognition technology, but also the impact that these tools have in expanding the ever-more present police state.

Conclusion

Evidence that facial recognition technology impedes civil and human rights has never been clearer. Even major technology companies have acknowledged the harms of law enforcement use of facial recognition. In June 2020, as institutions across the country faced a reckoning over racial equity, IBM, Microsoft, and Amazon announced they would halt the sales of their facial recognition technology to law enforcement.

Given the serious and undeniable threat that facial recognition technology poses, especially to Black and Brown people and other marginalized communities, we urge Congress to act swiftly to ensure that law enforcement does not have another tool to disproportionately discriminate against our most vulnerable communities. We look forward to working closely with this subcommittee to address the serious concerns with this technology.

²⁵ Julie Carr Smyth, *States Push Back Against Use of Facial Recognition by Police*, Associated Press (May 5, 2021), <https://apnews.com/article/race-and-ethnicity-health-coronavirus-pandemic-business-technology-e4266250f7e2d691d4d664735c2c6bc0>.

Ms. JACKSON LEE. Thank you very much for your testimony, and as well for that insightful constitutional analysis, which is extremely important.

Now, I would like to recognize Ms. Kara Frederick for five minutes.

STATEMENT OF KARA FREDERICK

Ms. FREDERICK. Chair Nadler, Chair Jackson Lee, Ranking Member Jordan, Ranking Member Biggs, thank you for the opportunity to testify today.

In four years, a projected six billion people will have access to the internet, with 80 billion devices connected to the Web. This creates profound digital surveillance opportunities. Facial recognition is a standout capability.

Some uses of facial recognition comprise legitimate public safety imperatives—finding the Capital Gazette shooter, as the Chair mentioned, and detecting individuals using fake passports. The potential for abuse by agents of the State is also high. Risks are manifold, like inaccurate algorithms and data security vulnerabilities.

I want to focus on three risks in particular.

- (1) The circumscription of civil liberties and individual privacy. The FBI is leading the way in the use of facial recognition for domestic surveillance. Today, the Bureau has access to over 640 million photos, in some cases through the use of private companies that scrape social media sites unbeknownst to the subject.
- (2) Outsourcing that surveillance to unaccountable private companies. Reports that the Biden Administration intends to expand the use of private companies unencumbered by constitutional strictures and with a history of reckless privacy practices are troubling.

Although government entities, like DHS, have long used private firms to identify patterns in publicly available information, a renewed push to make use of outside expertise for domestic spying on the heels of the new White House plan to counter domestic extremism portends potential Fourth Amendment concerns.

Such impulses to outsource domestic surveillance can lead to more expansive monitoring by law enforcement, which leads to the third risk:

- (3) The potential integration of facial recognition data with other PII through the expansion of mass surveillance.

The technical capabilities are already here. Now, multiple data sources can be aggregated and synchronized to allow governments to look for patterns in citizens' behavior. Faster networks with lower latency provide quick transmission and higher throughput to handle increased data flows.

More compute power and options, along with developments in machine learning and analytics that extract value from data, all fit together in mutually reinforcing ways, combining to weave diverse data streams into a grid of total surveillance if desired.

This can engender a climate of fear, self-censorship, and the chilling of free speech and the right to peaceably assemble in public places.

While authoritarian powers like China are at the bleeding edge of using facial recognition for internal control, the demonstrated inclination by governments to expand these powers in democratic na-

tions renders the slope a slippery one. We know that once these powers expand, they almost never contract.

The trend lines are foreboding. The United States nearly matches China in its surveillance coverage with one camera for every 4.6 people compared to China's one for 4.1 individuals.

Municipalities are using COVID as justification for expanded surveillance, as in the case of Peachtree Corners, Georgia, which became the first U.S. city to use AI-driven smart cameras to monitor social distancing and the use of masks this year.

Combined with near-historic low levels of public trust in the government to do what is right, the unfettered deployment of these technologies will continue to strain the health of the body politic without immediate and genuine safeguards.

Technology has long outpaced our efforts to govern it. To constrain abuse and bound expansion, Congress should establish a Federal data protection framework with appropriate standards and oversight for how U.S. user data is collected, stored, and shared by Federal, State, and local entities.

The initial focus of the effort should establish clear policies on data retention, categorize biometric surveillance data as sensitive data, and limit interoperability and data integration practices to stymie mass surveillance.

Congress should ensure that U.S. identity management systems are secure and reliable, based on proper standards and measurements, and in accordance with NIST guidelines. Programmers should build in data privacy protections in the design phase, testing new methods of encryption or differential privacy, decentralized models of data storage, or federated models of machine learning for these systems.

In sum, the debate over public safety and privacy trade-offs in our Republic provides an opportunity for us to embed technology with privacy protections from the outset and to shore up a system of checks and balances to address privacy infringements that do occur.

We are balanced on a razor's edge. How we decide to use and safeguard these technologies today either draws us closer to the free and open Republic we should be or closer to the authoritarian states whose surveillance practices we profess to abhor.

I look forward to taking your questions.

[The statement of Ms. Frederick follows:]



CONGRESSIONAL TESTIMONY

Facial Recognition Technology: Examining Its Use by Law Enforcement

Testimony before Subcommittee on Crime, Terrorism, and Homeland Security¹

United States House of Representatives

July 13, 2021

Kara Frederick
Research Fellow, Technology Policy
The Heritage Foundation

My name is Kara Frederick. I am a Research Fellow for Technology Policy at The Heritage Foundation. The views I express in this testimony are my own and should not be construed as representing any official position of The Heritage Foundation.

Background

Technology has long outpaced attempts to govern it. Facial recognition technology (FRT) is no different. In a world saturated with sensors, a projected 6 billion people with access to the Internet will generate between 80 zettabytes and 90 zettabytes of data worldwide by 2025.² In four years, approximately 80 billion devices will be connected to the Web, creating profuse surveillance opportunities.³ Nearly every facet of the daily life of an individual is already logged and captured—wittingly and unwittingly—by the sensors and digital applications in the new information environment.

And the barriers to entry are becoming lower and lower. In April 2019, *The New York Times* built a facial recognition “machine”—on the back of Amazon’s commercial facial recognition service—that detected more than 2,750 faces in a nine-hour period, in a single park in the New York City

borough of Manhattan alone, for approximately \$60.⁴

Federal and state government agencies—particularly law enforcement—have wasted no time harnessing this potential. From 2011 to 2019, an internal FBI unit that provides facial recognition capabilities facilitated 390,186 searches of 153,636 photos.⁵ A 2021 Government Accountability Office report indicated that 20 out of 42 federal agencies that employ law enforcement officers own or use FRT systems.⁶

The expansion of such use will continue as a stated public safety imperative. Specifically, FRT is currently used for entry at borders (Global Entry), Transportation Security Administration checkpoints (CLEAR), and more than 20 sports stadiums. Certain applications are legitimate: Success stories include the detection of Maryland’s *Capital Gazette* shooter in 2018 and the detention of at least three individuals using false passports at Dulles International Airport in the Washington, DC, area that same year.⁷

But the potential for abuse by agents of the state is high. Risks include: false positives generated by inaccurate algorithms, data security vulnerabilities to hacks and leaks, curtailment of civil liberties and

CONGRESSIONAL TESTIMONY

individual privacy, the outsourcing of surveillance to unaccountable private companies, and the potential integration of facial recognition data with other personally identifiable information through the expansion of mass surveillance.

Technical Challenges and False Positives

FRT development is beset with technical challenges. These systems repeatedly misidentify minorities, deliver high false-positive rates, and evince algorithmic bias. In 2020, a test by the National Institute of Standards and Technology (NIST) revealed higher false positive rates for African American females among existing facial recognition algorithms.⁸ The same test also discovered higher false match rates for Asian and African American faces relative to images of Caucasians. An earlier NIST test revealed that these systems misidentify African Americans at rates five to 10 times higher than white individuals.⁹ As such, an over-reliance on imperfect technology can lead to wrongful scrutiny and potential violations of individual liberties.¹⁰

Data Security

Extensive use of FRT systems makes data security risks—vulnerability to hacks and leaks—of heightened concern due to the immutable nature of biometrics. In 2019, Department of Homeland Security subcontractor Perceptics was subject to a “malicious cyber attack,” which compromised approximately 184,000 traveler images from the Customs and Border Patrol’s facial recognition pilot program. At least 19 of these images were posted to the dark web.¹¹ In the United Kingdom in 2019, hackers exploited a biometric security firm Suprema’s tool Biostar 2, spilling facial recognition data and other biometric data into the open.¹² Surveillance start-up Clearview AI, with its more than 2,400 law enforcement partners, also admitted in February 2021 that its client list was hacked.¹³

Civil Liberties and Individual Privacy

Regarding individual liberties, the FBI is leading the way in the use of FRT for domestic surveillance through its Facial Analysis, Comparison, and Evaluation (FACE) Services Unit and the Next Generation Identification–Interstate Photo System (NGI-IPS).¹⁴ Such pervasive use raises questions over undue privacy infringements. In just one example, an FBI special agent used a facial

comparison tool to scan a suspect’s girlfriend’s social media accounts which led to the suspect’s arrest in connection with the January 6th event at the Capitol over three months later. To expand the hunt for American citizens in the Capitol on January 6th, local law enforcement ran 129 facial recognition searches through Miami’s police team alone in response to the FBI’s call for investigative leads in early January.¹⁵ The private company employed by these Miami police, Clearview AI provides the ability to sift through its 3 billion image database scraped from social media sites and other corners of the Internet. On January 7th, Clearview AI saw their searches increase 26 percent.¹⁶

Outsourcing Surveillance and the Fourth Amendment

Reports that the Biden Administration intends to expand its outsourcing of domestic surveillance to private companies and contractors¹⁷ unencumbered by constitutional strictures are also troubling.¹⁸ Although government entities like the Department of Homeland Security have long used firms like social media aggregator Babel Street to identify patterns in publicly available information, a renewed push to “make use of outside expertise” for domestic spying portends potential Fourth Amendment violations.¹⁹ Further, scandals such as IBM’s 2019 use of millions of photos from unwitting citizens on the photo hosting site Flickr should not engender public trust in this type of data collection by private companies.²⁰ After a challenge from the American Civil Liberties Union (ACLU), even Twitter and Facebook cut off social media monitoring start-up Geofeedia’s access to their products in 2016 due to its invasive practices.²¹

Mass Surveillance

Such impulses to expand and outsource domestic surveillance can lead to more pervasive methods of monitoring by law enforcement. Multiple data sources can be aggregated and synchronized to allow governments to look for patterns in citizen’s behavior, and even potentially identify political dissidents. Now, faster networks with lower latency like 5G provide quick transmission and higher throughput to handle increased data flows. More compute power and compute options, such as cloud or edge computing, to sort and process the data are advancing in concert. Developments in machine

CONGRESSIONAL TESTIMONY

learning and sophisticated analytics that extract value from data are also growing exponentially.²² These improvements fit together in mutually reinforcing ways. Smart city initiatives may eventually combine these developments into regional panopticons that monitor citizens at the municipal level.

Indeed, the United States is currently testing plans for the basic building blocks of large-scale surveillance. Before the initiative was abandoned under public pressure in 2021, the City of Baltimore announced the deployment of a pilot program for wide-area motion imagery in December 2019, which would provide nearly 90 percent coverage of the city with three aircraft flying simultaneously. Baltimore Police Commissioner Michael Harrison claimed Baltimore would be “the first American city to use this technology in an attempt to solve and deter violent crime.”²³ Similarly, predictive policing, or the use of large data sets to predict and attempt to prevent crime “upstream” of its execution, is used in dozens of American cities via the California-based company PredPol.²⁴

Even municipalities without a law enforcement remit in the United States are getting in on the game, using the COVID-19 pandemic as a justification for the deployment of expanded surveillance measures. In early 2021, Peachtree Corners, Georgia, became the first U.S. city to use AI-driven “smart” cameras to monitor social distancing and use of masks.²⁵

Technical issues, hard cyber vulnerabilities, and the impulse to expand surveillance notwithstanding, FRT systems—especially *live* systems—are easily abused for political aims (e.g., to monitor political dissenters at rallies or individuals based on their ethnic makeup).

This political targeting using FRT is already demonstrable worldwide. Facial recognition purveyed the path for ethnic targeting in the western region of Xinjiang by Chinese authorities, where 1.5 million Uighers are imprisoned in reeducation camps, often through the use of FRT systems.²⁶ In Hong Kong, democratic protesters fearing a Chinese-style surveillance state cover their faces and use lasers to thwart monitoring by police.²⁷ In Russia, officials reportedly used FRT to identify and

arrest dissidents, including journalists, professors, and photographers, at April 2021 protests in support of the now-detained Russian opposition leader Alexei Navalny.²⁸

While authoritarian powers like China are at the bleeding edge of using FRT for internal control, the demonstrated inclination by governments to expand these powers in democratic nations renders the slope a slippery one. Right now, the United States’ system offers guardrails against such use in the form of sufficient rule of law protections, openness, a free press, independent judiciary, and engaged citizenry. For example, a wave of grassroots bans against the use of facial recognition by government entities materialized in 2019 and 2020. As of January 2020, 10 state legislatures introduced bills to limit, study, or generally increase transparency surrounding the use of facial recognition.²⁹ Cities in California like Oakland and San Francisco, as well as Massachusetts municipalities like Brookline, Somerville, and Cambridge have enacted bans on the use of facial recognition technology by local law enforcement and city officials.³⁰ And as of early 2020, Indiana, Maryland, Michigan, New Hampshire, New Jersey, South Carolina, and Washington were considering varying forms of restrictions and regulation.³¹ The ACLU is suing Clearview AI, and its Illinois arm filed a 2018 lawsuit against the Chicago Police Department to publicize its use of social media monitoring software.³²

However, trendlines are foreboding. The United States nearly matches China in its surveillance coverage, with one camera for every 4.6 people, compared to China’s one for 4.1 individuals.³³ Other Western democracies are expanding their use of surveillance technologies with an eye toward harnessing the latest tech developments. In January 2020, the United Kingdom’s Metropolitan Police force announced it would use Live Facial Recognition to immediately identify potential suspects in real time, employing technology in areas “where intelligence suggests [they] are most likely to locate serious offenders.”

Combined with near-historic low levels of public trust in the U.S. government to do “what is right,” the unfettered deployment of these technologies by

CONGRESSIONAL TESTIMONY

government entities will continue to strain the health of the body politic without immediate and genuine safeguards.³⁴

The Way Forward

To further distance itself from such practices and mitigate abuse, programmers in the United States should design with privacy in mind and continue to improve face recognition algorithms in order to mitigate false positives and increase accuracy. *We must take the time to get it right.*

To govern these technologies, U.S. lawmakers should incentivize transparency and openness, including data security and privacy protection laws that standardize collection, retention, and sharing of user data. The debate over public safety and privacy trade-offs in our republic provides an opportunity for the United States to articulate the right way to embed technology with privacy protections from the outset, in addition to maintaining a strong system of checks and balances to redress privacy infringements that do occur.

To constrain abuse and bound expansion by government agencies, a secure and privacy-protecting framework for the use of digital data obtained by FRT is requisite. To do so, Congress should:

Establish a federal data protection framework with appropriate standards and oversight for how U.S. user data is collected, stored, and shared by government entities—federal, state, and local—that use FRT. This framework should incentivize consistent, open, and transparent data practices by all law enforcement agencies. The initial focus of the effort should:

- Establish clear policies on data retention, such as time limits and the prohibition of infinite data storage.
- Categorize biometric data as “sensitive data” with additional protections, including limited interoperability to compartmentalize access between state and local law enforcement and federal entities, as well as between individual law enforcement bodies.

Similar measures should be taken to stymie data integration practices with other government-collected, shared, stored, transferred or purchased biometric data to prevent mass surveillance.

Ensure any U.S. identity management system used by government actors is secure and reliable, based on proper standards and measurements, and in accordance with NIST guidelines.³⁵

- Mandate built-in data privacy protections for U.S. identity management systems. This “privacy by design” concept builds in safeguards for users in the design phase of technology development. This can be done by utilizing new methods of encryption and/or differential privacy, decentralized models of data storage, or federated models of machine learning for these systems.³⁶
- Test and evaluate specific algorithms used by these entities on an annual basis to mitigate false positives and help increase accuracy.³⁷
- Consider recommendations that require NIST to share false-positive rates for minority groups when using one-to-many algorithms and when one photo is compared to many photos to identify a potential lead, as recommended by Heritage Foundation Visiting Fellow Brian E. Finch.³⁸

Enforce data protection inspections and oversight among all parties.³⁹

Update current timelines for publishing and updating all federal agencies’ Privacy Impact Assessments and System of Records Notices to require dissemination every six months of program use. Submit efficacy reports on the use of FRT systems by government entities and results (e.g., wrongful arrest rates and generation of investigative lead that led to successful prosecution, etc.)

CONGRESSIONAL TESTIMONY

The Heritage Foundation is a public policy, research, and educational organization recognized as exempt under section 501(c)(3) of the Internal Revenue Code. It is privately supported and receives no funds from any government at any level, nor does it perform any government or other contract work.

The Heritage Foundation is the most broadly supported think tank in the United States. During 2018, it had hundreds of thousands of individual, foundation, and corporate supporters representing every state in the U.S. Its 2018 operating income came from the following sources:

Individuals 67%
 Foundations 13%
 Corporations 2%
 Program revenue and other income 18%

The top five corporate givers provided The Heritage Foundation with 1% of its 2018 income. The Heritage Foundation's books are audited annually by the national accounting firm of RSM US, LLP.

¹The concepts and recommendations throughout this testimony are drawn from the author's previous working papers and publications, including but not limited to: Center for a New American Security, "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem," September 3, 2020, <https://www.cnas.org/publications/reports/the-razors-edge-liberalizing-the-digital-surveillance-ecosystem> (accessed July 12, 2021), and Center for a New American Security, "Democracy by Design," December 15, 2020, <https://www.cnas.org/publications/reports/democracy-by-design> (accessed July 12, 2021), as well as the author's media appearances from 2019–2021.

²David Reinsel, Jon Gantz, and John Rydning, "Data Age 2025: The Digitization of the World From Edge to Core," International Data Corporation *White Paper* No. US44413318, November 2018, <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf> (accessed July 12, 2021), and News release, "The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast," International Data Corporation, June 18, 2019, <https://www.idc.com/getdoc.jsp?containerId=prUS45213219> (accessed July 12, 2021).

³David Goldfein, keynote address, Air Force Association Air Warfare Symposium Orlando, Florida, February 23, 2018, https://www.af.mil/Portals/1/documents/csa/CSAF_AFA_Orlando-23Feb18.PDF (accessed July 12, 2021), and Gil Press, "IoT Mid-Year Update from IDC and Other Research Firms," *Forbes*, August 5, 2016, <https://www.forbes.com/sites/gilpress/2016/08/05/iot-mid-year-update-from-idc-and-other-research-firms/#16ec3e8355c5> (accessed July 12, 2021).

⁴According to *The New York Times* article, not every one of the 2,750 faces detected is necessarily unique. Sahil Chinoy, "We Built an 'Unbelievable' (but Legal) Facial Recognition Machine," *The New York Times*, April 16, 2019, <https://www.nytimes.com/interactive/2019/04/16/opinion/https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html/facial-recognition-new-york-city.html> (accessed July 12, 2021).

⁵Gretta L. Goodwin, Director Homeland Security and Justice, "Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains," testimony before the Committee on Oversight and Reform, U.S. House of Representatives, June 4, 2019, <https://www.gao.gov/assets/gao-19-579t.pdf> (accessed July 12, 2021).

⁶Government Accountability Office, "Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks," GAO-21-518, June 29, 2021, p. 1, <https://www.gao.gov/products/gao-21-518> (accessed July 12, 2021).

⁷U.S. Customs and Border Patrol, "Dulles CBP's New Biometric Verification Technology Catches Third Impostor in 40 Days," October 2, 2018, <https://www.cbp.gov/newsroom/national-media-release/dulles-cbp-s-new-biometric-verification-technology-catches-third> (accessed July 12, 2021).

⁸National Institute of Standards and Technology, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects," NISTIR 8280, December 2019, <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST-IR.8280.pdf> (accessed July 12, 2021).

CONGRESSIONAL TESTIMONY

- ⁹Tom Simonite, "The Best Algorithms Struggle to Recognize Black Faces Equally," *Wired*, July 22, 2019, <https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/> (accessed July 12, 2021).
- ¹⁰Kashmir Hill, "Wrongfully Accused by an Algorithm," *The New York Times*, June 24, 2020, <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html> (accessed July 12, 2021).
- ¹¹Office of the Inspector General for Homeland Security, "Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot," OIG-20-71, September 21, 2020, <https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf> (accessed July 12, 2021).
- ¹²Chris Baraniuk, "Biostar Security Software 'Leaked a Million Fingerprints,'" *BBC*, August 14, 2019, <https://www.bbc.com/news/technology-49343774> (accessed July 12, 2021).
- ¹³Clearview AI: Face-collecting company database hacked," *BBC*, February 27, 2020, <https://www.bbc.com/news/technology-51658111> (accessed July 12, 2021).
- ¹⁴Congressional Research Service, "Federal Law Enforcement Use of Facial Recognition Technology," *Report for Congress*, R46586, October 27, 2020, <https://fas.org/sgp/crs/misc/R46586.pdf> (accessed July 12, 2021).
- ¹⁵Drew Harwell and Craig Timberg, "How America's Surveillance Networks Helped the FBI Catch the Capitol Mob," *The Washington Post*, April 2, 2021, <https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/> (accessed July 12, 2021).
- ¹⁶Kashmir Hill, "The Facial-Recognition App Clearview Sees a Spike in Use after Capitol Attack," *The New York Times*, January 9, 2021, <https://www.nytimes.com/2021/01/09/technology/facial-recognition-clearview-capitol.html> (accessed July 12, 2021).
- ¹⁷The role of private tech companies in the development and use of facial recognition systems, especially as they contract with law enforcement agencies, cannot be overlooked. These companies currently possess the talent, data, and know-how to make the biggest leaps in technological progress on FRT. Duty, pushes for transparency must also be focused on and conducted with these companies in mind, not solely targeted at government agencies. In fact, according to a Pew study released in 2019, Americans are actually *more* suspicious of what private companies will do with facial recognition than they are of law enforcement. More than half of American adults trust law enforcement to use facial recognition responsibly, compared to the 36 percent that trust tech companies to do so. Aaron Smith, "More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly," Pew Research Center, September 5, 2019, <https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/> (accessed July 12, 2021).
- ¹⁸Zachary Cohen and Katie Bo Williams, "Biden Team May Partner with Private Firms to Monitor Extremist Chatter Online," *CNN*, May 3, 2021, <https://www.cnn.com/2021/05/03/politics/dhs-partner-private-firms-surveil-suspected-domestic-terrorists/index.html> (accessed July 12, 2021).
- ¹⁹Ibid.; Ken Dilanian and Julia Ainsley, "DHS Weighing Major Changes to Fight Domestic Violent Extremism, Say Officials," *NBC*, March 25, 2021, <https://www.nbcnews.com/politics/national-security/dhs-weighing-huge-changes-fight-domestic-violent-extremism-say-officials-n1262047> (accessed July 12, 2021); and Maya Villaseñor, "The Wild West of Smartphone Data and Surveillance," *Council on Foreign Relations*, February 1, 2021, <https://www.cfr.org/blog/wild-west-smartphone-data-and-surveillance> (accessed July 12, 2021).
- ²⁰Olivia Solon, "Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped without Consent," *NBC News*, March 12, 2019, <https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921> (accessed July 12, 2021).
- ²¹Jonah Engel Bromwich, Daniel Victor, and Mike Isaac, "Police Use Surveillance Tool to Scan Social Media, A.C.L.U. Says," *The New York Times*, October 11, 2016, <https://www.nytimes.com/2016/10/12/technology/aclu-facebook-twitter-instagram-geofeedia.html> (accessed July 12, 2021), and Curtis Waltman, "Meet Babel Street, the Powerful Social Media Surveillance Used by Police, Secret Service, and Sports Stadiums," *VICE*, April 17, 2017, https://www.vice.com/en_us/article/gv7g3m/meet-babel-street-the-powerful-social-media-surveillance-used-by-police-secret-service-and-sports-stadiums (accessed July 12, 2021).
- ²²Kara Frederick, "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem," *Center for a New American Security*, September 3, 2020, <https://www.cnas.org/publications/reports/the-razors-edge-liberalizing-the-digital-surveillance-ecosystem> (accessed July 12, 2021).
- ²³Tim Prudente, "Federal Appeals Court Rebukes Baltimore Spy Plane Program," *The Washington Post*, June 25, 2021, https://www.washingtonpost.com/local/legal-issues/baltimore-spy-plane-court-ruling/2021/06/25/f61e972c-d5c8-11eb-9f29-e96c9e843c6_story.html (accessed July 12, 2021).
- ²⁴Caroline Haskins, "Dozens of Cities Have Secretly Experimented With Predictive Policing Software," *VICE*, February 6, 2019, <https://www.vice.com/en/article/d3m7jq/dozens-of-cities-have-secretly-experimented-with-predictive-policing-software> (accessed July 12, 2021).

²⁵Alex Whittler, "Peachtree Corners Installs Cameras to Monitor Use of Masks, Social Distancing," Fox News, January 20, 2021, <https://www.fox5atlanta.com/news/peachtree-corners-installs-cameras-to-monitor-use-of-masks-social-distancing> (accessed July 12, 2021).

²⁶Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," *The New York Times*, April 14, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioscodebook&stream=technology (accessed July 12, 2021).

²⁷Paul Mozur, "In Hong Kong Protests, Faces Become Weapons," *The New York Times*, July 26, 2019, <https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html> (accessed July 12, 2021).

²⁸Ilya Arkhipov and Jake Rudnitsky, "In Moscow, Big Brother Is Watching and Recognizing Protesters," Bloomberg, May 2, 2021, <https://www.bloomberg.com/news/articles/2021-05-02/in-moscow-big-brother-is-watching-and-recognizing-protesters> (accessed July 12, 2021).

²⁹Kate Conger, Richard Fausset, and Serge F. Kovaleski, "San Francisco Bans Facial Recognition Technology," *The New York Times*, May 14, 2019, <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html?smty=cur&smid=tw-nytimes> (accessed July 12, 2021); Sarah Ravani, "Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns," *The San Francisco Chronicle*, July 17, 2019, <https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php> (accessed July 12, 2021); Sarah Wu, "Somerville City Council Passes Facial Recognition Ban," *The Boston Globe*, June 27, 2019, <https://www.bostonglobe.com/metro/2019/06/27/somerville-city-council-passes-facial-recognition-ban/SfaqQ7mG3DGulXonBHSCYK/story.html> (accessed July 12, 2021); and Nathan Sheard, "Victory: Brookline Votes to Ban Face Surveillance," Electronic Frontier Foundation, December 20, 2019, <https://www.eff.org/deeplinks/2019/12/victory-brookline-votes-ban-face-surveillance> (accessed July 12, 2021).

³⁰Ibid.

³¹Ibid.

³²American Civil Liberties Union, "ACLU Sues Clearview AI," May 28, 2020, <https://www.aclu.org/press-releases/aclu-sues-clearview-ai> (accessed July 12, 2021), and American Civil Liberties Union, "ACLU of Illinois v. City of Chicago," June 21, 2018, <https://www.aclu-il.org/en/cases/aclu-illinois-v-city-chicago> (accessed July 12, 2021).

³³Frederick, "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem."

³⁴Pew Research Center, "Public Trust in Government: 1958-2021," May 17, 2021, <https://www.pewresearch.org/politics/2021/05/17/public-trust-in-government-1958-2021/> (accessed July 12, 2021).

³⁵Kara Frederick, Center for a New American Security, "How Corporations and Big Tech Leave Our Data Exposed to Criminals, China, and Other Bad Actors," testimony before Judiciary Subcommittee on Crime and Terrorism, U.S. Senate, November 5, 2019, <https://www.judiciary.senate.gov/imo/media/doc/Frederick%20Testimony.pdf> (accessed July 12, 2021).

³⁶Richard Fontaine and Kara Frederick, "Democracy's Digital Defenses," *The Wall Street Journal*, May 7, 2021, <https://www.wsj.com/articles/democracys-digital-defenses-11620403161> (accessed July 12, 2021).

³⁷Congressional Research Service, "Federal Law Enforcement Use of Facial Recognition Technology," R46586, October 27, 2020, p. 11, <https://fas.org/sgp/crs/misc/R46586.pdf> (accessed July 12, 2021).

³⁸Brian E. Finch, "Addressing Legitimate Concerns About Government Use of Facial Recognition Technologies," Heritage Foundation *Legal Memorandum* No. 274, October 30, 2020, <https://www.heritage.org/civil-rights/report/addressing-legitimate-concerns-about-government-use-facial-recognition>.

³⁹Frederick, "How Corporations and Big Tech Leave Our Data Exposed to Criminals, China, and Other Bad Actors."

Ms. JACKSON LEE. Thank you very much for your testimony. We're now able to recognize Professor Laurin for five minutes.

STATEMENT OF JENNIFER E. LAURIN

Ms. LAURIN. Chair Jackson Lee, Chair Nadler, Ranking Member Biggs, Ranking Member Jordan, and Members of the Subcommittee, thank you very much for the opportunity to address the Subcommittee on the topic of facial recognition technology.

I will speak to a small but important sliver of this vast and complex topic that intersects with my own research and teaching on forensic science and criminal investigation and adjudication. The three bottom line points I want leave you with are these.

- (1) Although facial recognition technology matches have not been held to be admissible as evidence in criminal cases, law enforcement use of facial recognition to identify suspects does form the basis for arrests, criminal convictions, and periods of incarceration in the Federal and State systems.
- (2) While facial recognition has the capacity to be highly accurate under ideal conditions, there is greatest cause for concern about accuracy when used in criminal investigations.
- (3) That the criminal legal system is not itself well-designed to screen out mistaken or unreliable fruits of facial recognition technology.

To begin with the first point, facial recognition technology does lead to deprivations of liberty. Courts do not currently admit testimony or other evidence of facial recognition matches to establish that a defendant is the perpetrator of a crime.

However, evidence of facial recognition matches has been relied upon by courts in stages of criminal cases that are not governed by rules of admissibility, for example, in bail hearings to support decisions ordering pretrial detention, and in sentencing to find facts that enhance a defendant's sentence.

Perhaps more critically, the overwhelming majority of criminal prosecutions begin and end with no presentation of evidence before a jury at all. I refer, of course, to the nearly 98 percent of Federal criminal convictions obtained through guilty pleas.

In those cases, given the decidedly low evidentiary threshold of probable cause to arrest, facial recognition-generated matches can generate a criminal conviction without any courtroom testing of the government's evidence.

Moreover, even when facial recognition is used by law enforcement only to generate an initial lead, that early facial recognition match has the potential, particularly given the stickiness of cognitive biases and the very real potential for facial recognition matches to influence subsequent identifications, as Professor Friedman indicated, the capacity to send investigators down an erroneous path that even if ultimately corrected has enormous consequence for a wrongly accused individual like Mr. Williams.

The fact that facial recognition is shaping outcomes in criminal investigation and adjudication would be of little concern if there were no reason to question its accuracy as a means of identifying suspects. As others have already noted today, despite significant advances, significant concerns remain about facial recognition's accuracy.

There are at least two reasons why the criminal investigative context raises special worries.

- (1) As has already been discussed, the fact that there is significant variability and accuracy among facial recognition vendors, paired with the disturbing GAO findings that Federal agencies rely on a wide variety of—and sometimes unknown—facial recognition systems, points to an urgent need for disclosure of and perhaps restriction on what public and private facial recognition systems are being used.
- (2) Aside from variability and disparity in accuracy across algorithms, law enforcement use of facial recognition to identify criminal suspects raises special accuracy concerns because it is particularly likely that less than ideal images will be used in such procedures.

Studies of facial recognition that find low error rates do so only when using cooperative staged images. Declines in accuracy are consistently seen when using images not captured under ideal circumstances, precisely the types of images that are used in criminal investigations.

Finally, none of this might give rise to a need for legislative intervention if the criminal legal system already possessed adequate means to police investigative use of facial recognition. It does not.

Partly, this is due to the fact that as long as facial recognition matches are used as investigative tools and not relied on as evidence in a criminal case, there's little opportunity for a defendant who is identified to challenge that practice in court.

Additionally, however, restricted discovery, the sharing of case information between the prosecution and defense, means that defendants are severely hobbled in litigating law enforcement use of facial recognition.

In contrast to the regime in an increasing number of States, defendants in Federal criminal cases do not have access to the government's investigative file. Indeed, defendants might not even learn that an early facial recognition match procedure was performed.

Moreover, the trial-based timing of disclosure in Federal criminal cases means little opportunity exists for the defense to vet the reliability of government evidence before entering a plea.

Additionally, to date, defense claims that they are constitutionally entitled to information about facial recognition under the holding of the case *Brady v. Maryland* have gained little or no traction in courts.

In sum, facial recognition is an alluring forensic tool with potential to accurately open otherwise unavailable investigative avenues. Troublingly, the Federal criminal legal system is not well-designed to smoke out questionable uses of the technology.

I look forward to your questions.

[The statement of Ms. Laurin follows:]

**Opening Statement of Professor Jennifer Laurin, Wright C. Morrow Professor of Law,
The University of Texas School of Law**

“Facial Recognition Technology: Examining Its Use by Law Enforcement”

Subcommittee on Crime, Terrorism, and Homeland Security

July 13, 2021

Chairwoman Jackson-Lee, Ranking Member Biggs, Chairman Nadler, Ranking Member Jordan, and Members of the Subcommittee on Crime, Terrorism, and Homeland Security –

Thank you very much for the invitation to address this subcommittee on the subject of facial recognition technology, or “FRT.” This is a vast and complex topic – concerning technology, criminal law, constitutional law, business and intellectual property, and more. I will address a small but important sliver of that vast landscape that intersects with my own research and teaching on forensic science and criminal investigation and adjudication. The three bottom line points that I want to leave you with are these: First, although FRT “matches” have not been held to be admissible in evidence in criminal cases, law enforcement use of FRT to identify suspects forms the basis for arrests, criminal convictions, and periods of incarceration in the federal system; second, while FRT has the capacity to be highly accurate under ideal conditions, there is *greatest* cause for concern about accuracy when used in criminal investigations; and third, that the criminal legal system is not well-designed to screen out mistaken or unreliable fruits of facial recognition technology.

To begin with the first point: FRT does lead to deprivations of liberty. Courts do not currently admit testimony or other evidence of FRT matches to establish that a defendant is the perpetrator of a crime, and my understanding is that federal prosecutors maintain that they do not seek to use such evidence in their case-in-chief. Nevertheless, evidence of FRT matches has been relied upon by federal courts in stages of criminal cases that are not governed by rules of admissibility – for example, in bail hearings to support decisions ordering pretrial detention of the defendant, and in sentencing to find facts that enhance a defendant’s sentence.¹ Perhaps more critically, the overwhelming majority of criminal prosecutions begin and end with no presentation of evidence before a jury at all; I refer of course to the nearly 98% of federal criminal convictions obtained through guilty plea.² In those cases, and given the designedly low evidentiary threshold of probable cause to arrest, FRT-generated matches can generate a criminal conviction without any courtroom testing of the Government’s evidence to prove the defendant’s identity. Moreover, even where FRT is used by law enforcement only to generate an initial lead, that early FRT match has the potential – particularly given the stickiness of cognitive biases – to

¹ See, e.g., *United States v. Lee*, 451 F. Supp. 3d 1, 4 (D.D.C. 2020); *United States v. Jones*, No. 16 CR. 121 (RWS), 2017 WL 3049543, at *3 (S.D.N.Y. Jul. 18, 2017).

² *United States Sentencing Commission, Fiscal Year 2020 Overview of Federal Criminal Cases* (Apr. 2021), https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2021/FY20_Overview_Federal_Criminal_Cases.pdf.

send investigators down an erroneous path that, even if ultimately corrected, has enormous consequence for a wrongly accused individual.³

The fact that FRT is shaping outcomes in criminal investigation and adjudication would be of little concern if there were no reason to question its accuracy as a means of identifying suspects. But as others have already noted today, despite significant advances that have improved the accuracy of FRT, significant concerns remain. There are at least two reasons why the criminal investigative context raises special worries about what we know about the reliability of FRT to identify individuals – particularly in performing what are known as “one-to-many” database searches. First, as the National Institute of Standards and Technology reported in its July 2021 Face Recognition Vendor Test, there remains significant variability in accuracy among FRT vendors based on different algorithms used for comparing known and unknown faces.⁴ Particularly given the results of the GAO’s recent survey of federal agencies, reporting that across and within agencies investigators are relying on a wide variety of different FRT systems,⁵ this accuracy variability points to a need for disclosure of and perhaps restriction on what public and private FRT systems are being utilized. Second, aside from variability and disparities in accuracy across systems and algorithms, law enforcement use of FRT to identify criminal suspects raises special accuracy concerns because it is particularly likely that less-than-ideal images will be used in such procedures. Studies of FRT that find low error rates do so only when using cooperative, front-facing, staged images; declines in accuracy are consistently seen when using side-view images, low-resolution images, or other images not captured under controlled circumstances – precisely the types of images that are often used in criminal investigations in which the perpetrator’s identity is not yet known.⁶ Thus, while FRT is understandably viewed by law enforcement as a powerful investigative tool, the criminal investigative context is in fact one of the most challenging settings in which to reliably deploy the technology.

None of this might give rise to a need for legislative intervention if the criminal legal system already possessed adequate means to police, as it were, investigative use of FRT. For a variety of reasons, it does not. Partly, this is due to the fact that as long as FRT matches are used as investigative tools and not themselves relied on as evidence in a criminal case, there is little opportunity for a defendant who is identified through use of FRT to challenge that practice in court – there is no evidence to suppress or the admissibility of which to litigate. Additionally, however, restrictive discovery – the sharing of case information between the prosecution and

³ See Jennifer E. Laurin, *Remapping the Path Forward: Toward a Systemic View of Forensic Science Reform and Oversight*, 91 Tex. L. Rev. 1051, 1096—97 (2013).

⁴ National Institute of Standards and Technology, NISTIR 8721 Draft Supplement (Jul. 7, 2021), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.

⁵ U.S. Government Accountability Office, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks* (Jun. 2021), <https://www.gao.gov/assets/gao-21-518.pdf>.

⁶ National Institute of Standards and Technology, NISTIR 8721 Draft Supplement (Jul. 7, 2021), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.

defense – means that defendants are severely hobbled in litigating law enforcement use of FRT. In contrast to the regime in an increasing number of states, defendants in federal criminal cases do not have access to all – or even much – of the Government’s investigative file.⁷ Indeed, defendants might not even learn that an early FRT match procedure was performed. Moreover, the trial-based timing of disclosure in federal criminal cases means that little opportunity exists for defense attorneys to learn of and vet the reliability of Government evidence before entering a plea. Additionally, to date, defense claims that they are constitutionally entitled to information about FRT procedures under the holding of the case *Brady v. Maryland*, have gained little or no traction in courts.⁸ And, to the extent that meaningful vetting of FRT reliability requires probing the details of the algorithms generating match sets, the fact that many FRT systems are proprietary creates additional trade-secret barriers to disclosure of such information.⁹ These are just some of the reasons why the adversarial adjudicatory setting is poorly structured to test the reliability of FRT used by federal investigators.

In sum, FRT is an alluring forensic tool that has the potential to accurately open otherwise unavailable investigative avenues, but also has the potential to inject a new source of error into criminal adjudication. Troublingly, the federal criminal legal system is not well-designed to smoke out questionable uses of FRT through the ordinary operation of processing criminal cases – making consideration of other means of regulation and oversight especially necessary.

⁷ See Fed. R. Crim. P. 16.

⁸ 373 U.S. 83 (1963).

⁹ See generally Rebecca Wexler, *Life, Liberty, and Trade Secrets*, 70 Stan. L. Rev. 1343 (2018).

Ms. JACKSON LEE. Thank you very much, Professor, for your testimony.

Now, I recognize Mr. Brett Tolman for five minutes. Mr. Tolman, you are recognized. Thank you.

STATEMENT OF BRETT TOLMAN

Mr. TOLMAN. Thank you, Chair Jackson Lee, Ranking Member Biggs, and Members of the Subcommittee. Thanks for the opportunity to testify today.

My name is Brett Tolman. I'm the Executive Director of Right on Crime, a conservative organization dedicated to the promotion of criminal justice policies that promote public safety, individual liberty, and whole communities. I've previously served as United States Attorney, as a Federal prosecutor, and as chief counsel for crime and terrorism for the United States Senate Judiciary Committee.

The first issue to address is concerning lack of transparency and basic information relating to law enforcement's use of facial recognition technology. Many of the fundamental questions that you likely want and deserve answers to, are currently unanswerable, questions, simple questions, such as how many law enforcement entities use facial recognition? How often do they use it? Who is in their databases and why?

Beyond those Federal law enforcement agencies, one might suspect of using facial recognition, like the FBI, there are a host of others with less apparent need who also use the technology. For example, the U.S. Fish and Wildlife Service and the Internal Revenue Service.

Also, discomfiting are the sources of the photos supporting this technology. For example, the government utilizes millions of photos of law-abiding individuals collected from driver's licenses and passports; but private technology companies that contract with law enforcement have harvested billions of photos posted by unsuspecting users on platforms such as Facebook, YouTube, and even Venmo. This collection is an unprecedented invasion of privacy that places enormous undue control in the hands of the government and Big Tech, two entities not always known for their light touch or responsible use of power.

Walking out the door in the morning can be an exercise in skipping from one camera to another. To this perpetual passive surveillance, law enforcement can potentially add recordings from body worn cameras and the Smartphone in an officer's pocket.

In short, there are very few instances where law enforcement will not have the opportunity to subject a person of interest to facial recognition technology.

Inevitably, the first temptation will be, and has been, to use facial recognition by default rather than necessity. Instead of limiting the practice to serious public safety risks or only after due process has been afforded an individual, officers may use and have already used the practice for run-of-the-mill interactions in minor cases.

Our Founding Fathers deliberately and prudently enshrined in the Bill of Rights prescriptions on the wanton search of Americans as a necessary bulwark for freedom. It is hard to square those notions and protections with the unfettered use of a technology that

can instantaneously reveal an individual's identity as well as potentially their association and prior movements. The unrestricted use of facial recognition bears little difference to allowing police to collect fingerprints or DNA from anyone and everyone they come across, an abuse that we clearly do not and should not tolerate.

Furthermore, we cannot ignore the risk that facial recognition technology will be used to target certain Americans. Facial recognition can instantly strip away the anonymity of crowds and ultimately threaten our constitutional rights of assembly and association. Consider the chilling effect facial recognition could have if used to identify individuals at a political rally or a government protest.

This practice grossly lacks accountability. Right now, we have little more than vague assurances that we should trust the government to safely use the incredible power of facial recognition technology without such information or oversight.

Not long ago, I was tasked with leading the effort in the United States Senate to reauthorize the PATRIOT Act. We heard similar assurances years ago by those leading the Department of Justice and the FBI about FISA and those surveillance authorities not being turned against honest Americans. We have seen how that worked out as outlined in the recent and disturbing Inspector General reports. None of this is to say that law enforcement should never have access to facial recognition technology.

While China's unconscionable use of facial recognition technology to enhanced and accelerated its undemocratic control of its citizenry is a warning of the cost of failure, I do not believe it is an inevitable consequence of any use of facial recognition technology by law enforcement.

Further, it is unrealistic to expect law enforcement officials to permanently deny themselves a tool that is increasingly prevalent in the commercial sector and which has such powerful capacity to improve public safety. It is easy to contrive a scenario in which we would very much want law enforcement to have this technology, searching for a known terrorist loose in our city presenting an eminent risk to the public, or seeking to identify a mass murder suspect, for example.

However, acknowledging there are credible uses for facial recognition technology and voicing support for law enforcement is not the same as writing a blank check for power and then looking the other way. If nothing else, we need a reset in which law enforcement agencies must gain affirmative permission from relevant, democratically elected representatives to use this technology prior to its use. That way transparency, accountability, and proper use guidelines can be established.

I look forward to answering your questions.

[The statement of Mr. Tolman follows:]



Testimony

July 13, 2021

Facial Recognition Technology: Examining Its Use by Law Enforcement

*Testimony before the United States House of Representatives
Committee on the Judiciary*

by Brett Tolman, Executive Director

Chair Jackson Lee, Ranking Member Biggs, and Members of the Subcommittee on Crime, Terrorism, and Homeland Security:

Thank you for the opportunity to testify today.

My name is Brett Tolman, and I am the Executive Director of Right on Crime, a conservative organization dedicated to the promotion of criminal justice policies that promote public safety, individual liberty, and whole communities. I have previously served as the United States Attorney for the District of Utah, as an Assistant United States Attorney, and as Chief Counsel for Crime and Terrorism for the United States Senate Judiciary Committee. The past decade I have also worked in private practice as the founder of the Tolman Group, focusing on government reform, criminal defense, and internal corporate investigations, and previously as a Shareholder and Chair of the White Collar, Corporate Compliance and Government Investigations Section of the law firm of Ray Quinney & Nebeker, PC.

I am encouraged by the Subcommittee's decision to hold a hearing today on the use of facial recognition technology by law enforcement entities. It is an area of increasing concern that is ripe for abuse and could stand to benefit from congressional attention and oversight.

The first issue to address is a concerning lack of transparency and basic information relating to law enforcement's use of facial recognition technology. Many of the fundamental questions that you likely want—and deserve—answers to are currently unanswerable. Questions such as: How many law enforcement entities use facial recognition? How often do they use it? Who is in their databases and why?

To the extent that we have partial answers to some of these questions, the facts are daunting. Recently, the Government Accountability Office revealed that beyond those federal law enforcement agencies one might suspect of using facial recognition, like the Federal Bureau of Investigation, there are a host of others with less apparent need who also use the technology. For example, the U.S. Fish and Wildlife Service and the Internal Revenue Service.¹ Nationally, one estimate placed the government market for facial recognition in this country at \$136.9 million in 2018, with the expectation that it would nearly triple by 2025.² Another estimate suggested that as of 2016, at least 1 in 4 police departments had the option to run facial recognition searches, a number that has surely grown since then.³

Also disconcerting are the sources of the photos supporting this facial recognition technology. In addition to drawing on pictures secured through the criminal justice process, the government utilizes millions of photos of law-abiding individuals collected for driver's licenses and passports.⁴ Private technology companies that contract with law enforcement have harvested billions of photos posted by unsuspecting users on platforms such as Facebook, YouTube, and even Venmo.⁵ This collection is an unprecedented invasion of privacy that places enormous, undue control in the hands of the government and Big Tech, two entities not always known for their light touch or responsible use of power.

¹ <https://www.gao.gov/assets/gao-21-518.pdf>

² <https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251>

³ <https://www.perpetuallineup.org/>

⁴ <https://www.gao.gov/assets/gao-16-267.pdf>

⁵ <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>

continued

Mass surveillance compounds the issues surrounding mass collection. Walking out the door in the morning can be an exercise in skipping from one camera to another, as everywhere from the convenience store on the corner to the traffic camera at the light in front of it record our actions. To this perpetual passive surveillance, law enforcement can potentially add recordings from body-worn cameras or simply from the smartphone in an officer's pocket. In short, there are very few instances where law enforcement will *not* have the opportunity to subject a person of interest to facial recognition technology.

Inevitably, the first temptation will be to use facial recognition by default rather than necessity. Instead of limiting the practice to serious public safety risks or only after due process has been afforded an individual, officers may use—and have already used—the practice for run-of-the-mill interactions and minor cases.⁶ Our Founding Fathers deliberately and prudently enshrined in the Bill of Rights proscriptions on the wanton search of Americans as a necessary bulwark for freedom. It is hard to square these notions and protections with the unfettered use of a technology that can instantaneously reveal an individual's identity as well as potentially their associations and prior movements. The unrestricted use of facial recognition bears little difference to allowing police to collect fingerprints or DNA from anyone and everyone they come across, an abuse that we clearly do not, and should not, tolerate.

The implications of such access to personal information become especially troubling when dealing with real-time interactions between law enforcement and members of the public. Americans have long prided themselves on our ability to refuse the government unless it has legitimate cause to interfere with our liberty. Our police, at least in the absence of reasonable suspicion of wrongdoing or additional judicial process, are supposed to rely on the consent of the citizenry in their interactions. Facial recognition has the power to stand this principle on its head and turn questions from law enforcement about personal information into mere rhetorical ones.

In addition to identifying individuals, facial recognition technology makes it much easier for law enforcement to track them. It can essentially automate surveillance across the network of cameras mentioned above, following individuals with minimal effort or oversight. It could also mean historical tracking. Once somebody lands on law enforcement's radar, there is little stopping officers from running their image through available videos and photos to reconstruct past days, their associations or affiliations, and other aspects of their life or routine.

Furthermore, we cannot ignore the risk that facial recognition technology will be used to target certain Americans. Facial recognition can instantaneously strip away the anonymity of crowds, and ultimately threaten our constitutional rights of assembly and association. Consider the chilling effect facial recognition could have if used to identify individuals at a political rally or government protest. This technology could be used to identify everyone who simply visits a gun store or any other place an individual is exercising a personal freedom or choice that a particular politician or other individual heading an agency considers undesirable.

This practice grossly lacks the necessary accountability. Right now, we have little more than vague assurances that we should trust the government to safely use the incredible power of facial recognition technology without such information or oversight. Not long ago, I was tasked with leading the effort in the Senate to reauthorize

⁶ <https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251>

the PATRIOT Act. We heard similar assurances years ago, by those leading the Department of Justice and the FBI about FISA and those surveillance authorities not being turned against honest Americans. We have seen how that worked out as outlined in the recent, and disturbing, Inspector General reports.

None of this is to say that law enforcement should *never* have access to facial recognition technology. While China's unconscionable use of facial recognition technology to enhance and accelerate its undemocratic control of its citizenry is a warning of the costs of failure, I do not believe it is the inevitable consequence of any use of facial recognition technology by law enforcement. Further, it is unrealistic to expect law enforcement officials to permanently deny themselves a tool that is increasingly prevalent in the commercial sector and which has such powerful capacity to improve public safety. It is easy to contrive a scenario in which we would very much want law enforcement to have facial recognition technology available—searching for a known terrorist loose in one of our cities presenting an imminent risk to the public, or seeking to identify a mass-murder suspect, for example. And while I harbor a conservative's healthy skepticism of government, I respect members of law enforcement and will always seek to support them and their mission to keep us all safe. However, acknowledging there are credible uses for facial recognition technology and voicing support for law enforcement is not the same as writing a blank check for power and then looking the other way.

In the past, members of this Subcommittee and others in Congress have proposed a moratorium on the use of facial recognition technology by law enforcement. Significant restraints might be necessary for privacy protections to catch up to the rapidly advancing capabilities of this technology. If nothing else, we need a reset in which law enforcement agencies must gain affirmative permission from relevant democratically elected representatives to use this technology prior to its use; that way transparency, accountability, and proper use guidelines can be established.

As it stands, it is difficult to see how the regular, widespread use of this technology can meet the high standards of our Constitution and its protection of civil liberties or the norms inherent in a democratic society. If one considers this technology as creating the ability to find a needle in a haystack, it seems entirely reasonable to demand the police to first know which needle they are looking for, rather than search every haystack in the off chance it contains a needle. Absent an emergency or other exceptional circumstance, some manner of reasonable suspicion should likely be a prerequisite to a facial recognition search. Likewise, we should be exceedingly cautious about the deployment of real-time facial recognition, which has more disturbing Fourth Amendment implications. Finally, we need transparency on when, how, and why every law enforcement agency is using facial recognition and which databases they are drawing from, and we should have particular reticence when it comes to the collection of images from unwitting, law-abiding individuals.

This is a pressing issue pertaining to all Americans' fundamental rights. As someone who has spent a great deal of time working on legislation in this arena and someone who fundamentally believes that smaller government is better government, I am encouraged that the Subcommittee is concentrating its focus on these concerns today. I expect that its resolution will require many conversations, careful balancing of tradeoffs, and potentially difficult decisions. I look forward to contributing however I can to that effort today. Thank you once again, Chair Jackson Lee, Ranking Member Biggs, and other Members of this Subcommittee. ★

ABOUT THE AUTHOR



Brett L. Tolman is the founder of the Tolman Group and the executive director for Right on Crime. He is dedicated to state and federal policy and advocacy, especially on criminal justice reform. Prior to entering private practice, Tolman was appointed by President George Bush in 2006 as the United States Attorney for the District of Utah and held that office for nearly 4 years from 2006-2009. As U.S. Attorney for Utah, he was responsible for cutting-edge cases addressing such issues as international adoption fraud, mortgage fraud, international marriage fraud, sex and human trafficking, terrorism, and breaches of national security. In 2009 he handled the prosecution of Brian David Mitchell, the convicted kidnapper of Elizabeth Smart. From 2008-2009 he was selected by Attorney General Michael Mukasey to serve as special advisor to the attorney general on national and international policy issues affecting United States attorneys and the Department of Justice. Prior to his appointment as U.S. Attorney, Tolman served as chief counsel for crime and terrorism to the United States Senate Judiciary Committee.

During his career, Tolman has testified multiple times in the United States Congress and assisted in drafting and passing many pieces of legislation affecting state and federal criminal justice systems. These include the First Step Act of 2018, the Corrections Act, the Sentencing Reform Act, the Justice for All Act of 2004, Protection of Lawful Commerce in Arms Act (2005), the Violence Against Women and Department of Justice Reauthorization Act of 2005, the USA Patriot Improvement and Reauthorization Act of 2005, and the Adam Walsh Protection and Safety Act (2006). He is a frequent contributor on Fox News, CNN, MSNBC, NewsMax and *No Spin News* with Bill O'Reilly.

About Right on Crime

Right on Crime is a national campaign of the Texas Public Policy Foundation, in partnership with the American Conservative Union Foundation and Prison Fellowship, which supports conservative solutions for reducing crime, restoring victims, reforming offenders, and lowering taxpayer costs. The movement was born in Texas in 2007, and in recent years, dozens of states such as Georgia, Ohio, Kentucky, Mississippi, Oklahoma, and Louisiana, have led the way in implementing conservative criminal justice reforms.



Ms. JACKSON LEE. Mr. Tolman, we thank you for your testimony. It's now my pleasure and privilege to recognize Dr. Cedric Alexander for five minutes.

Dr. Alexander, you are recognized.

STATEMENT OF CEDRIC L. ALEXANDER

Dr. ALEXANDER. Thank you, and good morning, Madam Chair, and those who are Ranking Members and Subcommittee Members, for the opportunity to be here with you. I hail from the great State of Florida, Pensacola more specifically, so it's great being here with you.

I'm going to try not to be redundant, because maybe some of what I'm going to say has already been mentioned in the time that has been allocated; but let me start by saying this: On July 9, Portland, Maine Press Herald reported on two newly enacted acts, laws that make Maine the first U.S. State to enact a broad ban on government use of facial recognition technology.

In Maine, State, county, and municipal governments will not be allowed to use any sort of FRT. Law enforcement may use the technology for investigating certain serious crimes, but State law enforcement agencies are barred from implementing their own FRT systems. They may request FRT searches from the FBI and the State Bureau of Motor Vehicles in certain cases.

A year earlier, in August of 2020, the Portland City Council totally banned the use of facial recognition by the police. Indeed, currently there are approximately 24 American cities that ban police FRT use, and many other organizations has called for a nationwide ban because of evidence that false positive identification in the case of people of color exceed the rate of Whites. So, the Federal Government has enacted no law on how law enforcement may or may not use facial recognition technology.

The benefits of facial recognition systems for policings are quite evident. Some have already been mentioned here. It is, in fact, that technology that does aid in the detection and prevention in crime. For an example, facial recognition is effectively used for issuing identity documents and is usually combined with long-accepted biometric technologies, such as fingerprints and iris scans.

FRT face matching is used at border checks to compare the portrait of digitized biometric passports, and FRT, as we all know, was used to identify suspects in the January 6 violent breach of the U.S. Capitol, and high-definition digital photograph and videography, sometimes deployed from aerial drones may be used increasingly to identify faces in mass events.

Currently, the FBI's a leading law enforcement agency that uses FRT, and it has developed technology and best practices to promote the intelligent use of technology to reduce error and protect constitutional rights.

In addition, the Facial Identification Scientific Working Group operating under the National Institute of Standards and Technology Organization of Scientific Area Committees is working to develop standards for facial recognition technology. Facial recognition technology has been useful and law enforcement, I believe, will continue to develop technically and, therefore, become even more useful. Blanket bans on FRT in policings are unwarranted and

deny to police agencies a tool that is important to aid in public safety.

Make no mistake, there are urgent constitutional issues relating to privacy protection from unreasonable searches, due process, and the presumption of innocence. Especially concerning are false positives and negative identification results.

In addition, police do not always use FRT correctly. For instance, on May 16, 2019, *The Washington Post* reported that some agencies use altered photos, forensic art sketches, and even celebrity look-alikes for facial recognition searches. In one case, the Post's Drew Hall wrote, "New York police detectives believed a suspect looked like the actor Woody Harrelson." So, they ran the actor's image through a search and then arrested a man that system had suggested might be a match. Forgive me for being blunt, but that was pretty, pretty egregious, quite frankly.

Using artificial technology to confer upon a highly subjective visual impression, a halo of digital certainty is neither fact-based, prudent, efficient, or just. Under Federal law, at least it is not illegal for the simple reason that no Federal laws govern the use of facial recognition.

I'm going to stop here and be more than glad to answer any questions that you may have, particularly from a very practical perspective as being a former chief in two major cities in this country, and a former Federal security director for the U.S. Department of Homeland Security in Dallas, Texas, for 5.5 years. So, I understand the importance of this technology, but I also understand how it could be easily abused if those are not properly trained, certified in the utilization and best practices are not evident.

So, thank you, Madam Chair.

[The statement of Dr. Alexander follows:]

Issues in Facial Recognition in Law Enforcement**Statement by Dr. Cedric L. Alexander**

On July 9, the Portland, Maine, *Press Herald* reported on two newly enacted laws that make Maine the first US state to enact a broad ban on government use of facial recognition technology. In Maine, state, county, and municipal governments will not be allowed to use any sort of FRT. Law enforcement may use the technology for investigating certain serious crimes, but state law enforcement agencies are barred from implementing their own FRT systems. They may request FRT searches from the FBI and the state Bureau of Motor Vehicles in certain cases.

A year earlier, in August 2020, the Portland City Council totally banned the use of facial recognition by the police. Indeed, currently some 24 American cities ban police FRT use, and Black Lives Matter has called for a nationwide ban because of evidence that false positive identifications in the case of people of color exceed the rate for whites. So far, the federal government has enacted no laws on how law enforcement may or may not use FRT.

The benefits of facial recognition systems for policing are quite evident. It is a fact that the technology can aid in the detection and prevention of crime. For example:

- Facial recognition is effectively used when issuing identity documents and is usually combined with other long-accepted biometric technologies, such as fingerprints and iris scans.

- FRT face matching is used at border checks to compare the portrait on digitized biometric passports.
- In the United States, at least 26 states (perhaps more) permit law enforcement to run searches against their databases of driver's license and ID photos. (The FBI has access to the driver's license photos of 18 states.)
- FRT was used to identify suspects in the January 6 violent breach of the U.S. Capitol, and high-definition digital photograph and videography (sometimes deployed from aerial drones) may be used increasingly to identify faces in mass events.
- Facial recognition closed-circuit TV systems may be used in such public security missions as finding missing children and disoriented adults, identifying and tracking criminals and criminal suspects, and generally supporting and accelerating investigations.

Currently, the FBI is the nation's leading law enforcement agency using FRT, and it has developed technologies and best practices to promote the intelligent use of the technology to reduce errors and protect constitutional rights. In addition, the Facial Identification Scientific Working Group (FISWG), operating under National Institute of Standards and Technology (NIST) Organization for Scientific Area Committees, is working to develop standards in FRT.

Facial recognition technology has been useful in law enforcement and, I believe, will continue to develop technically and therefore become even more useful. Blanket bans on FRT in policing are unwarranted and deny to police agencies a tool that is an important aid to public safety.

But make no mistake. There are urgent constitutional issues relating to privacy, protection from unreasonable search, due process, and the presumption of innocence. Especially concerning are false positive and negative identification results. Although a Customs and Border Patrol (CBP) internal analysis found a false positive rate that compared favorably with identifications made directly by human observers, a late 2019 NIST study confirmed that FRT accuracy does vary by demographic factors, including age, sex, and race. And, yes, false positives are higher for Asian and African American faces compared to those of Caucasians.

In addition, police do not always use FRT correctly. For instance, on May 16, 2019, *The Washington Post* reported that some agencies use altered photos, forensic artist sketches, and even celebrity look-alikes for facial recognition searches. “In one case,” the *Post*’s Drew Harwell wrote, “New York police detectives believed a suspect looked like the actor Woody Harrelson, so they ran the actor’s image through a search, then arrested a man the system had suggested might be a match.”

Forgive my being blunt. But this is stupid.

Using artificial intelligence to confer upon a highly subjective visual impression a halo of digital certainty is neither fact-based, prudent, efficient, nor just. But, under federal law, at least, it is not illegal—for the simple reason that no federal laws govern the use of facial recognition.

Absent federal laws—or even a fully developed professional and legal consensus—states are beginning to fill the legislative vacuum. In some cases, they are doing so by simply banning all police use of FRT.

What we really need is intelligent policy and legislation, beginning with a requirement for transparency. At present, very few law enforcement agencies disclose how and how frequently they use FRT. Even fewer audit their personnel for improper use of facial recognition systems. Most departments have no internal oversight or accountability mechanism to detect misuse. Secrecy in matters of constitutional rights, human rights, and civil rights provokes fear and suspicion.

And it should.

Like so many digital technologies, facial recognition was not long ago the stuff of science fiction. Today, many of us carry it in our pockets in the form of a smartphone that recognizes our face when we take it out to make a call or send a text. FRT has become a normal part of 21st-century living. I believe that most Americans are willing to accept that facial recognition can be a valuable tool in law enforcement. But without the judicious and just application of *human* intelligence, including full-disclosure transparency, public accountability, prudent legislation, and science-based regulation and best practices guidance, the technologies of *artificial* intelligence are not tools. They are blunt instruments. And we all know that blunt instruments can become weapons. We cannot afford to sacrifice constitutional rights on the one hand or, on the other, a technology that can promote justice and even save lives.

Ms. JACKSON LEE. Dr. Alexander, thank you and thank you to all the Witnesses. We obviously have opened up in the parochial and often used term, nonlegal, a can of worms that we need to certainly address.

We will now be able to proceed with Members questions, and I'm very grateful for the attendance to all you Members, both on the minority side, and as well on the majority.

We will now proceed under the five-minute rule with questions.

I will now begin by recognizing myself for five minutes.

Director Goodwin, you obviously know of the report, the GAO report of 2019, indicating that facial recognition algorithms tested accuracy in a real way by race, ethnicity, or country of origin, as well as gender, and it differed in accuracy.

What are some of the concerns related to facial recognition system accuracy, Director?

Dr. GOODWIN. Thank you for that, Madam Chair.

So, a number of concerns have been raised around the report around accuracy, and I will just focus on the main one. So, just in terms of if you think about a person's face, it's distinct; it typically doesn't change. If a person's face is—that information is breached or hacked, that is totally different than your password being breached. Well, you can change your password, but you cannot change your face.

So, in the report, we note this particular concern. The misidentification based on a facial image is of great concern, and we note that in our report.

Ms. JACKSON LEE. Thank you very much.

Mr. Williams, you were wrongfully arrested in front of your wife and daughters, detained for 30 hours in a filthy, overcrowded detention center because of facial recognition. Your story is stunning, in particular holding up a picture alongside of your face, your good comment, "Do we all look alike?" You are a suspect allegedly in a theft investigation. Prosecutors dropped the charges, and the Detroit Police Chief apologized for sloppy detective work.

Tell us, what impact did your arrest and detention have on you and your family? You are obviously a gentleman with employment, a family. How did that impact you?

Mr. WILLIAMS. Ah, well, thank you. Well, the first thing when I came home was on the drive home, my wife was saying how she had to figure out how to get in contact with the detention center because they kept hanging up on her and telling her they can't answer any questions because they don't have any information. All they know is that I am there, and that is all they can tell her.

When I got home, I asked my wife what was going on, and my daughter had took family pictures of us and turned them around because she said she couldn't bear to look at me while I was in jail, and I had to go talk to a five-year old at the time about a mistake that had been made by the police, and she—it was hard to make her understand that sometimes they make mistakes because you tell her as a child that the police are your friend, and if you ever get in trouble, this is who you go to and this was going to help. I had to deal with that, and we have thought about even taking her to a psychiatrist, because when we replay the video from what

happened, she can't stand to watch it. She gets all emotional, and it's understandable. I have to go through that, I mean—

Ms. JACKSON LEE. Painful. Thank you so very much.

Mr. WILLIAMS. Yeah.

Ms. JACKSON LEE. Thank you so very much.

Professor Friedman, you have heard that story. My time is short, and I have one or two other questions.

What are the privacy implications and risk to communities if a private company has access to the details of law enforcement investigations? You might add your thought about a legislative fix or thought about how we address this question.

Professor Friedman?

Mr. FRIEDMAN. Thank you, Chair. That was an incredibly moving story. I have kids, and I can only imagine.

The problem, as I think Dr. Alexander pointed out, is that the use of this technology is a bit like the wild west. There's no regulation. When there's no regulation, we are going to have mistakes, and we are going to have breaches, and we are going to have all kinds of trouble. There are uses of the technology for law enforcement, but you need a full set of regulations.

I've set out a bunch of them in my testimony. I think you could do a lot of this by regulating the vendors directly. As a product moving in interstate commerce, you could set a number of standards, including that the companies themselves have to regulate and identify what are effective probe images, what are the right size of the databases, what are the thresholds to avoid false positives and false negatives under different circumstances, that the technology is self-auditing so that we could know what how it was actually used by law enforcement. So, there's a lot of things that can be done.

Ms. JACKSON LEE. Thank you very much.

Just, Dr. Alexander, what are your suggestions on how law enforcement authorities can reduce the phraseology that the Detroit chief had to acknowledge, sloppy detective work, without greatly reducing investigative efficacy?

Dr. Alexander?

Dr. ALEXANDER. Thank you, Madam Chair.

I guess having been a former chief and I had to respond in that way, that would certainly suggest to me that I have a larger systemic issue around the way investigations are conducted, and how people are interviewed.

Here's the issue, though, for me. The technology is one in which we use every day. We pick up our cell phone. We use it to access calls or text messages, whatever the case may happen to be. The biggest issue here for me, and will continue to be, when you have victims such as Mr. Robert Williams, people who are innocently going along their way, because of a failed ability for us in policing, quite frankly—and I say “we” because I have been there—the inability to train people appropriately. They have to be trained. There has to be certifications. There has to be best practices, and there needs to be certification both, I believe, certainly at a State level, and a Federal level, that has to be ongoing, because one thing that we know currently is that we don't train enough.

When you are utilizing that type of technology that can easily infringe upon someone's Fourth Amendment rights, I think we have to be very careful. We also have to remember where we came from, even in DNA technology, where we there, too, have seen over the years, particularly in the past, we have seen DNA labs that were shut down because of people's inability to carry out that professional function based on certification and accuracy. We don't want to find ourselves using this technology doing the same things that we have done in the past, because what it will continue to do, Congresswoman, is drive that proverbial wedge even further apart between good policing and communities across this country, and I don't think that is a road we want to continue to go around—to go down.

Ms. JACKSON LEE. Thank you so very much.

My time has expired. I know that there are many other questions that I have interest in, but let me yield to the Ranking Member of the Subcommittee, Mr. Biggs, for five minutes.

Mr. BIGGS. Thank you, Madam Chair.

Dr. Goodwin, thank you for being here today.

In your most recent report, you found that 13 of the 14 agencies that you surveyed that reported using non-Federal systems did not have complete, up-to-date information about what systems their employees were even using.

Is that a correct interpretation?

Dr. GOODWIN. Yes, that's correct, sir.

Mr. BIGGS. So, in fact, if I understand right, even one of the agencies you worked with had to poll its employees to see whether they were using the system, and what systems they were using. Is that accurate, too?

Dr. GOODWIN. That's correct, Congressman.

Then one of the agencies polled, yes, they initially told us that they didn't use the technology. When they polled their employees, they found that the technology had been used in over 1,000 searches.

Mr. BIGGS. Well, if agency leadership does not even know what systems their employees are using, or whether they are using it, how can they be sure that those systems are not being misused, and that our constitutional rights of American citizens are not being violated?

Dr. GOODWIN. So, this speaks to the heart of the recommendations that we made, that agencies have an awareness. It's important that they have an awareness of what systems they are using, particularly the non-Federal systems that their employees are using. Given that awareness, then they can then begin to ensure that the appropriate protections are in place related to privacy and accuracy.

Mr. BIGGS. Ms. Frederick, we know Federal agencies are using private searches, and they are collecting literally billions of images. How are those images acquired?

Ms. FREDERICK. Well, it depends on the private company. A lot of these companies—Clearview AI was mentioned earlier—they claim to scrape the Internet, social media sites, things you might upload, what your grandma is still using Flickr to upload. There's an IBM scandal there as well. So, they are basically just scraping

what is publicly available on the internet when people are unwittingly uploading these photos, clicking yes to some of the terms of use on these private companies. They are not consenting to allow these images to be used by law enforcement; but by using those non-Federal private companies, these contractors like Clearview AI, like Babel Street has been mentioned, they are just using your regular photos from your grandma, family, sisters, and your daughters. So, it is pretty much a government-infused wild west out there.

Mr. BIGGS. Mr. Tolman, these systems, these private systems—let's leave off Federal systems for a moment, or law enforcement systems—what steps are they even taking to secure their systems?

Mr. TOLMAN. Well, the reality is they are more interested in the dollars that are behind this technology than they are securing civil liberties, and that will always be the case. When private companies are contracting and utilizing a powerful technology, their interest is going to be driven by their bottom line.

Mr. BIGGS. So, Mr. Tolman, back to you still, these agencies, like Federal agencies that are using private services, is it just easier for them to contract out than to develop their own system, I assume?

Mr. TOLMAN. Yes. The capability is hundreds of millions of photos versus what they would be able to gather themselves with limited staff and resources.

Mr. BIGGS. So, how are we going to ensure that Americans are not being targeted by Federal agencies using the facial recognition technology? What are your policy prescriptions?

Mr. TOLMAN. So, there certainly is—as others have said, there's going to have to be a complete shift, meaning the legislature is going to have to enact regulations that require any agency, government agency, whether they are contracting or not with Big Tech or other companies, are going to have to have policy that allow for the proper use, the legal use of this, ones in which you all say is a legal use.

I prosecuted the kidnapper of Elizabeth Smart. I can imagine during that case, when I was a prosecutor, we would have clearly sought out law enforcement's ability to use that to identify Elizabeth and try to find her. That is a far cry than just downloading all from social media what you can and then targeting others without the legal justification or the regs or policies that have been approved by Congress.

Mr. BIGGS. Mr. Lee, I'm going to ask you the same question. What prescriptions, policy prescriptions do you advocate that we can ensure that Americans are not being targeted by Federal agencies or other law enforcement agencies?

Mr. LEE. Ranking Member Biggs, thank you for the question.

The Leadership Conference supports a ban, or moratorium, on the use of these technologies. We support a ban or moratorium because:

- (1) These communities are already—the communities where facial recognition technology is used are already over-policed and over-surveilled.
- (2) Facial recognition technology is disproportionately inaccurate for Black and Brown communities, particularly, communities of color.
- (3) The community has not been involved in these processes. Congress has not engaged in legislation on these topics. Communities have not been

involved in highlighting what they think policing should be, specifically within the context of facial recognition technology.

Mr. BIGGS. Thank you.

My time is up, Madam Chair. Thank you.

Ms. JACKSON LEE. Thank you very much.

Now, I'm pleased to recognize Mr. Nadler, Chair of the Committee.

Mr. Nadler, you are recognized.

Chair NADLER. Thank you, Madam Chair.

Director Goodwin, I would like to focus on the FBI's use of facial recognition technology. In your report, you found that 15 agencies reported using systems owned by another Federal entity, and 14 reported using systems owned by State, local, Tribal, or territorial entities, including the FBI.

Can you briefly describe for us how the FBI uses State systems to expand its facial recognition search capacity?

Dr. GOODWIN. Thank you, sir, for that question.

So, I will briefly talk about how the FBI used the technology around the events following the killing of George Floyd in May 2020.¹ So, the FBI has a media tip line, as I'm sure you are aware of, and so what they did, they asked for people to submit images to the media tip line. The images that were submitted to the tip line they then inserted into an FRT system to try to get some potential matches.

So, that is one way the FBI has used the technology.

We did a report a few years ago on FBI specific use of the technology, and we had issued a number of recommendations that spoke to them complying with the Privacy Impact Assessment, otherwise known as PIA, and the Systems of Record Notice, otherwise known as the SORN. The FBI—ultimately, they agreed with our recommendations, and they implemented the recommendations. So, they have—I think it was Dr. Alexander who mentioned that the FBI has done a number of things to ensure that the accuracy of the FRT systems that they are using has improved.

Chair NADLER. Thank you.

Also, Director Goodwin, your report describes how agencies use nongovernment-owned systems. What are the potential security risks associated with a Federal law enforcement agency using a non-Federal Government-owned, or, even a State- or local government-owned FRT system?

Dr. GOODWIN. So, I will focus on the non-Federal systems, and it's something that we speak to in the report. As I mentioned earlier, the Privacy Impact Assessments and the Systems of Record Notice, the PIA and the SORN, those are two standards that typically, if a government agency is using their own system, they have to follow. So, the concern that we mentioned in our report is that if they are using a non-Federal entity for facial recognition technology, that entity, that non-Federal entity may or may not have to comply with the recommendations and the guidelines laid out under the PIA and the SORN, and, so, that is a concern. So, with the PIA, that, of course, speaks to how the images are being used.

¹ Director Goodwin requested to update this sentence. The original statement was "So, I will briefly talk about how the FBI used the technology around the events of January 6."

The SORN speaks to the fact that if there's a change in the technology, that information has to be made public and available.

Chair NADLER. Thank you.

Professor Laurin, for those who are arrested following law enforcement officers' use of facial recognition technology to match them to a suspect's photo, what protections are in place for defendants, who are presumed innocent at that point, to challenge the use of the facial recognition technology that led to their arrest?

Ms. LAURIN. Well, in many instances today, it's quite limited, the opportunity to do that. In fact, practically nonexistent to the extent that the practice has been for law enforcement agencies to use the facial recognition match as a lead that then is corroborated through other evidence. The risk, though, is that that corroboration ends up not truly being independent corroboration.

So, for example, in a case in Florida, a facial recognition match was made based on an image in a store, and subsequently a police officer who knew that the match had been made, looks at the image himself and said, yeah, these two guys look alike. So, already knowing that the computer had assisted a match sort of doubled down on it, which is not an independent corroboration.

What courts have said is that defendants really don't have the right to challenge the facial recognition match when the government isn't relying on it in court; but that misses the fact that the match could taint what is showing up in court.

Chair NADLER. Thank you.

Facial recognition systems have been found to be less effective in detecting people of color and women. As we heard from Mr. Williams, he experienced this technological flaw in real time when he was misidentified despite his photo not resembling the suspect.

Professor Friedman and Mr. Lee, can facial recognition technology be incorporated fairly into criminal investigative and public safety strategies despite this inherent flaw in the algorithms?

Professor Friedman?

Mr. FRIEDMAN. Go ahead.

Mr. LEE. First, Chair, it's a pleasure to see you again, especially under these circumstances. Secondly, the Leadership Conference does not. Currently the issues of accuracy alone would say that—would hold that a ban or moratorium would be the most appropriate use. In addition, these technologies are being used in communities that are already over-policed and over-surveilled. So, there is no way to get around the accuracy and over-surveillance issues that come with law enforcement use of facial recognition technology.

Chair NADLER. Mr. Friedman?

Mr. FRIEDMAN. Chair, so I want to echo the grave concern about technologies that have these demographic differentials, as I said in the past, that they ought not be used unless that can be addressed. Actually, join Mr. Tolman in thinking strongly that we shouldn't be using the technologies until there's regulation. There may be ways to deal with the demographic disparities if we understand what they actually are, but we don't have that testing, so we have learning to do. Then, we have to think about what it means to have a human in the loop because many people offer that up as a way to ensure that these things don't go wrong. As Mr. Williams' story all

too graphically demonstrates, the way we use humans in the loop right now don't do that. It might be possible to develop protocols and best practices to do that; but we have not made that happen yet, and that is why we suggest that we need regulation.

Chair NADLER. Thank you.

Madam Chair, before I yield back, I ask unanimous consent to place the following into the record: A statement from over 40 civil rights groups, a letter from the Security Industry Association, and individual statements from Data for Black Lives, the Electronic Frontier Foundation, and the Project on Government Oversight.

Ms. JACKSON LEE. Without objection, so ordered.

[The information follows:]

CHAIR NADLER FOR THE RECORD



June 3, 2021

Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology

Across the country, local, state, and federal law enforcement and immigration agencies use face recognition systems to identify, track, and target individuals. More than half of all U.S. adults are already in face recognition databases used for criminal investigations.¹ This technology dramatically expands law enforcement's power and poses severe threats to everyone's safety, wellbeing, and freedoms of expression and association—but especially for Black and Brown communities, Muslim communities, immigrant communities, Indigenous communities, and other people historically and currently marginalized and targeted by policing.

Much of the public debate has focused on the alarming inaccuracy of face recognition systems, particularly on women and people with darker skin.² In at least three cases that are publicly known, police have relied on erroneous face recognition identifications to make wrongful arrests of Black men, underscoring the dangerous nature of this technology in the hands of law enforcement.³

But improvements in the technology's accuracy will not address the fundamental problem: face recognition expands the scope and power of law enforcement, an institution that has a long and documented history of racial discrimination and racial violence that continues to this day. In the context of policing, face recognition is always dangerous—no matter its accuracy. Throughout our nation's history, law enforcement has used surveillance to silence dissent and to maintain white supremacy, from slave patrols⁴ to the FBI's COINTELPRO program. Face recognition and other modern surveillance technologies promise to continue a history that has shown itself to be incompatible with the freedoms and rights of Black and Brown communities.

¹ Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Geo. L. Ctr. on Privacy & Tech. 42 (Oct. 18, 2016), available at <https://www.perpetuallineup.org/>.

² Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* (2018), available at <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>; Patrick Grother, Mei Ngan, Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280, Nat'l Inst. of Standards and Technology (December 2019), available at <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>.

³ Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. Times (Dec. 29, 2020), <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>.

⁴ Hassett-Walker, Connie, *The Racist Roots of American Policing: From Slave Patrols to Traffic Stops*, The Conversation (June 2, 2020), available at <https://theconversation.com/the-racist-roots-of-american-policing-from-slave-patrols-to-traffic-stops-112816>.

Given this history, it's no surprise that many law enforcement agencies have adopted face recognition technologies in secret, without the input or approval of policymakers or the public. In cases where the public has learned of an agency's use of face recognition, key details about how the system works and how it's used often remain concealed, even from criminal defendants. The details that have been uncovered to date are troubling: agencies often run searches on "flawed" face data—matches based on low confidence thresholds, artist-drawn composite sketches, and images that have been heavily edited.⁵ The undersigned groups agree that law enforcement's use of face recognition is invasive and harmful to all communities, with severe and disproportionate harms for Black and Brown communities.

The most comprehensive approach to addressing the harms of face recognition would be to entirely cease its use by law enforcement. The six concerns outlined below highlight why the strongest policy action on face recognition is urgently needed.

1. Regardless of technical accuracy, law enforcement use of face recognition systems could exacerbate the harms of policing in communities that are already targeted by the police.

Much attention has been focused on the increased errors in face recognition systems on Black and Brown people.⁶ But even if bias could be entirely eliminated from the technology, the use of face recognition will still disproportionately harm Black and Brown communities. This is because, as is the case with any practice or tool of policing, face recognition is more likely to be deployed on Black and Brown communities.⁷ As a consequence, the individuals subject to face recognition searches that may lead to targeting by police are disproportionately likely to be of color. In addition, law enforcement's use of mugshot databases for face recognition searches means that Black and Brown people, who are disproportionately targeted for arrest and

⁵ Despite the danger of such action causing errors and producing unreliable information, departments edit photos with computer generated imagery, use sketches, or even run scans on celebrity lookalikes in their face recognition systems. See Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data* (May 16, 2019), <https://www.flawedfacedata.com/>.

Additionally, some departments permit matches with low confidence thresholds—meaning a low certainty of the matching being accurate—to be used. For example, Amazon recommended a police department configure its systems to return matches with no minimum confidence threshold even after making public statements that police setting systems to return matches below 99 percent would be irresponsible. See, Jake Laperruque, *About-Face: Amazon's Shifting Story on Facial Recognition Accuracy*, The Project On Government Oversight (April 10, 2019), <https://www.pogo.org/analysis/2019/04/about-face-examining-amazon-shifting-story-on-facial-recognition-accuracy/>.

⁶ Patrick Grother, Mei Ngan, Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTIR 8280, Nat'l Inst. of Standards and Technology (December 2019), available at <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>.

⁷ One police department found that their use of face recognition on communities of color was up to 2.5 times greater than their proportion of the population being policed. See Automated Regional Justice Information System, San Diego's Privacy Policy Development: Efforts & Lessons Learned, 11, available at <https://drive.google.com/file/d/1ZR2jiiLcBMUKnHTRk1ZC248NbFUqNRww/view?usp=sharing>.

incarceration, will be more likely to show up in search results.⁸ In this manner, face recognition risks carrying forward historical biases and exacerbating existing biases in the way our communities are policed.

2. Law enforcement use of face recognition threatens individual and community privacy by allowing invasive and persistent tracking and targeting.

Face recognition is already a pervasive part of American policing. Law enforcement agencies routinely use the technology to compare an image from bystanders' smartphones, CCTV cameras, or other sources with face image databases maintained by local, state, and federal agencies. Potentially more than 133 million Americans are included in these databases, with at least thirty-one states giving police access to driver's license images to run or request searches,⁹ and twenty-one states giving the FBI access to the same.¹⁰ Law enforcement use of these databases for investigations places millions of Americans in what has been called a "perpetual line-up,"¹¹ posing particular risk to privacy and access to public space for Black and Brown people, immigrants, and other groups who are routinely targeted by police.

Face recognition, when used with persistent surveillance camera networks, further erodes anonymity in public spaces, allowing law enforcement to perpetually track the movements of nearly any person at any time. Major American cities have piloted persistent face surveillance, which continuously scans live video to identify individuals.¹² Such tracking undermines fundamental rights to association, expression, and privacy.¹³ The Supreme Court's 2018 decision in *Carpenter v. United States* held that warrantless location tracking using cell site location data for more than seven days is unconstitutional.¹⁴ Persistent face surveillance can "catalogue every single movement" of individuals in the same way, and it's arguable that such tracking would be unlawful under a *Carpenter* analysis.¹⁵

3. Law enforcement use of face recognition can chill First Amendment-protected activities.

⁸ See Clare Garvie, Alvaro Bedoya, Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Oct. 18, 2016), note 236, https://www.perpetuallineup.org/findings/racial-bias#footnote236_b52kvrq, <https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-GarvieC-20190522.pdf>.

⁹ Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Geo. L. Ctr. on Privacy & Tech. 42 (Oct. 18, 2016), available at <https://www.perpetuallineup.org/>.

¹⁰ *Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains*, Government Accountability Office (June 4, 2019), <https://www.gao.gov/products/GAO-19-579T>.

¹¹ Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Geo. L. Ctr. on Privacy & Tech. 42 (Oct. 18, 2016), available at <https://www.perpetuallineup.org/>.

¹² Clare Garvie and Laura Moy, *America Under Watch: Face Surveillance in the United States*, (May 16, 2019), <https://www.americaunderwatch.com>.

¹³ See, e.g., *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms.")

¹⁴ 138 S.Ct. 2206 (2018).

¹⁵ *Id.* at 2217, quoting *Jones* at 430 (Alito, J., concurring).

Face recognition presents a serious threat to First Amendment rights. Law enforcement can use face recognition to identify people attending large protests, political events, or religious ceremonies, and catalog individuals' engagement in these First Amendment-protected activities. American history is fraught with efforts to monitor individuals based on dissent¹⁶ or religious beliefs,¹⁷ and face recognition could supercharge that surveillance. The mere threat of face recognition being used to catalog, interfere with, or retaliate against First Amendment-protected activities will in itself chill participation and expression in a way that is not compatible with democratic society.¹⁸

In 2015, Baltimore police used face recognition amid protests against the police killing of Freddie Gray to find individuals with "outstanding warrants and arrest[ed] them directly from the crowd," in order to disrupt, punish, and discourage protesters.¹⁹ Police in cities including Washington, D.C.,²⁰ New York City,²¹ and Miami²² also used face recognition to identify protestors during the uprising against anti-Black racism and police violence in 2020. In addition to broad surveillance, face recognition can be too easily warped into a tool for selective prosecution. The ability to pull up face recognition matches for individuals with an active bench warrant for a low-level offense has already been abused to target those exercising their First Amendment rights. In most jurisdictions law enforcement agencies do not even need evidence of a crime committed in order to run a face recognition search. This broad-based face surveillance chills civic engagement and promotes self-censorship. While this threat is significant for existing face recognition technologies, it's even more significant for emerging forms of persistent face surveillance.

4. Law enforcement use of face recognition can easily violate due process rights and otherwise infringe upon procedural justice.

¹⁶ Senate Select Committee, Book III: Supplementary Detailed Staff Reports, 94th Cong., 2d sess., 1976, S. Rep. 94-755.

¹⁷ *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, The Muslim American Civil Liberties Coalition & The Creating Law Enforcement Accountability & Responsibility (CLEAR) Project at CUNY School of Law (2013), <https://www.law.cuny.edu/wp-content/uploads/page-assets/academics/clinics/immigration/clear/Mapping-Muslims.pdf>.

¹⁸ Ryan Calo, *The Boundaries of Privacy Harm* (July 16, 2010) at 16-17, *Indiana Law Journal*, Vol. 86, No. 3, 2011, available at <https://ssrn.com/abstract=1641487>.

¹⁹ Kevin Rector & Alison Knezevich, *Social Media Companies Rescind Access to Geofeedia, Which Fed Information to Police During 2015 Unrest*, *Balt. Sun* (Oct. 11, 2016), <https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html>.

²⁰ Justin Jouvenal & Spencer S. Hsu, *Facial Recognition Used To Identify Lafayette Square Protestor Accused of Assault*, *Wash. Post* (Nov. 2, 2020), https://www.washingtonpost.com/local/legal-issues/facial-recognition-protests-lafayette-square/2020/11/02/64b03286-ec86-11ea-b4bc-3a2098fc73d4_story.html.

²¹ James Vincent, *NYPD Used Facial Recognition to Track Down Black Lives Matter Activist*, *The Verge* (Aug. 18, 2020), <https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram>.

²² Kate Cox, *Cops in Miami, NYC Arrest Protestors From Facial Recognition Matches*, *Ars Technica* (Aug. 19, 2020), <https://arstechnica.com/tech-policy/2020/08/cops-in-miami-nyc-arrest-protesters-from-facial-recognition-matches/>.

New technologies, including face recognition systems, often allow law enforcement to circumvent existing legal protections for individuals. Due process requirements govern law enforcement actions throughout the criminal legal process, including stop-and-frisks, investigations, searches, arrests, and beyond. Yet, in the twenty years that face recognition has been used in some jurisdictions, defendants' rights to due process protections have been essentially non-existent when it comes to the technology.²³ And because prosecutors and law enforcement often conceal the use of face recognition in criminal trials, it may be difficult, if not impossible to ensure that defendants are able to exercise their Sixth Amendment rights.²⁴

The ability to assess the reliability of both the face recognition systems and the ways in which they are used is critical to ensuring due process of law. Protecting due process rights and preserving *Brady*²⁵ rights would require that law enforcement agencies disclose key details about the design and use of the system that impact the reliability of matches. This includes information about the make and model of the particular system used; the training data and inner workings of that system; and where, when, and how humans make decisions when using the system. Face recognition searches require a number of human decisions, each necessarily bringing in the discretion and subjectivity of the user. Depending on the choices made by the agent using the face recognition system at a number of steps throughout the process, the results of the face recognition system could vary greatly, producing different matches, and different potential evidence.²⁶ The person making these decisions is also likely the person who will assess matches generated by the system and make the ultimate decision of which is the "match." Because the decisions involved in running face recognition searches can have a profound impact on the process and outcome for those arrested, disclosure of information about each of these steps is important to ensuring the defendant is afforded due process.²⁷

Additionally, the right "to be confronted with the witnesses against him" found in the Sixth Amendment of the Constitution is a critical feature of a fair trial. Defendants have the right to cross examine the people involved in creating reports and witnesses who provide identification, and to investigate the tools and tests that provided evidence. Any evidence that is considered "testimonial" in a case should be subject to examination in order to uphold those rights. Face

²³ Jennifer Valentino-DeVries, *How The Police Use Facial Recognition, And Where It Falls Short*, N.Y. Times (Jan. 12, 2020), <https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html>.

²⁴ Karen Gullo & Jennifer Lynch, *When Facial Recognition Is Used to Identify Defendants, They Have a Right to Obtain Information About the Algorithms Used on Them*, EFF Tells Court, EFF.org (March 12, 2019), <https://www.eff.org/deeplinks/2019/03/when-facial-recognition-used-identify-defendants-they-have-right-obtain>.

²⁵ *Brady v. Maryland*, 373 U.S. 83 (1963). "The *Brady* Rule," or "*Brady* rights," as they are commonly known, require that prosecutors disclose materially exculpatory evidence in the government's possession to the defense.

²⁶ A face recognition system that leads to arrest, or any investigative or police action, could be impacted and made more or less reliable by a number of factors, including the confidence thresholds used and the dataset of photos used to train the system, and the photo provided to conduct the search. For example, the person running the search can manipulate the photo to make it more accessible to the technology by taking actions such as pasting in eyes, or even substituting an image of a famous actor, as some have done. See Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data* (May 16, 2019), <https://www.flawedfacedata.com/>.

²⁷ That disclosure should therefore also include information regarding what other matches the system returned.

recognition is increasingly used to identify the accused,²⁸ meaning that each step in the design and use of the technology must be disclosed in detail to defendants, who then have the right to challenge those procedures and algorithms in court. Complicating these issues, companies often make intellectual property claims to trade secrets to protect their algorithms and prevent their inner workings from coming to light, impeding defendants' rights to confront evidence in court.²⁹

²⁸ Kashmir Hill, *Wrongfully Accused By An Algorithm*, N.Y. Times (June 24, 2020), <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>; Jennifer Valentino-DeVries, *How The Police Use Facial Recognition, And Where It Falls Short*, N.Y. Times (Jan. 12, 2020), <https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html>.

²⁹ See, e.g., *Wisconsin v. Loomis*, 371 Wis.2d 235, 243 (Wisc. 2016).

5. Face recognition systems used by law enforcement often rely on faceprints that have been obtained without consent.

Developers of face recognition systems often use faceprints obtained without consent and in violation of public trust.³⁰ A prominent example is Clearview AI, which created a face recognition tool used by over 600 federal, state, and local law enforcement agencies and private companies across the country.³¹ To build its data set for matching faceprints, Clearview amassed over 3 billion faceprints by scraping photos from across the Internet, including employment sites, news sites, and social media networks such as Facebook, unbeknownst to the subjects of these images.³² While the well-known Clearview database is used for running searches, databases used to train face recognition models also often rely on faceprints obtained or used for this purpose without consent. For instance, IBM captured faceprints by annotating user-uploaded images from the photo sharing site Flickr with details like skin tone and facial geometry.³³ Additionally, in January 2021, the Federal Trade Commission settled with photo storage app Everalbum over its misuse of user photos for face recognition purposes, requiring Everalbum to delete face recognition models developed using user photos and videos.³⁴

In order to run face recognition searches, law enforcement relies on various sources including driver's license photos and mugshots. The faceprints used to identify possible matches have been collected without consent for that purpose. Many states will run searches against their driver's license photo databases for the FBI.³⁵ Additionally, states can submit images to the FBI to run against its own face recognition database, which includes mugshots submitted by federal, state, and local agencies. State and local law enforcement agencies also maintain and run searches against their own databases of driver's license and mugshot images from their own jurisdiction, as well as other jurisdictions and even other countries. For example, the Maricopa County Sheriff's Office in Arizona included mugshots from Honduras in its face recognition match database.³⁶

Using people's faceprints outside of their original purposes and without their knowledge is an invasion of privacy and violates public trust.

³⁰ Inioluwa Deborah Raji and Genevieve Fried, *About Face: A Survey of Facial Recognition Evaluation*, AAAI 2020 Workshop on AI Evaluation (Feb. 1, 2021), <https://arxiv.org/abs/2102.00813>.

³¹ Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020), <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

³² *Id.*

³³ Olivia Solon, *Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped Without Consent*, NBC News (March 12, 2019), <https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921>.

³⁴ Federal Trade Commission https://www.ftc.gov/system/files/documents/cases/everalbum_complaint.pdf JD Supra (January 20, 2021), <https://www.jdsupra.com/legalnews/alert-ftc-requires-app-developer-to-6691322/>.

³⁵ *Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains*, Government Accountability Office (June 4, 2019), <https://www.gao.gov/products/gao-19-579t>.

³⁶ Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Geo. L. Ctr. on Privacy & Tech. 42 (Oct. 18, 2016), available at <https://www.perpetual lineup.org/>.

6. In addition to racial bias in how law enforcement uses face recognition, the technology itself poses disproportionate risks of misidentification for Black, Asian, and Indigenous people.

Studies of face recognition algorithms have documented the fact that commercial algorithms available for purchase and used by government entities around the country have inequitable error rates across a number of demographics including race, sex, and age.³⁷ The National Institute of Standards and Technology's Face Recognition Vendor Test found significant variation in both false positive and false negative error rates³⁸ across race, sex, and age with the highest false positives for U.S. law enforcement mugshots among Black, Asian, and Indigenous people.³⁹ In a comparison of match rates by country of origin, photos of people from East African countries had false positive rates 100 times higher than the baseline rate.⁴⁰

CONCLUSION

The evidence that face recognition technology impedes our rights has never been more clear. Even major technology companies have acknowledged the harms of law enforcement use of face recognition. In June 2020, as institutions across the country faced a reckoning over racial equity, IBM, Microsoft, and Amazon announced that they would be halting the sales of their face recognition technology to law enforcement. Now is the moment for national policymakers to address law enforcement use of this technology.

A ban or moratorium on law enforcement use of face recognition is the most effective way to address all of the concerns outlined in this statement. With Congress slow to act, a number of states and localities have taken action. Over a dozen cities across the country have banned face recognition, and multiple states have placed restrictions on its use.⁴¹ Accordingly, it is essential that any federal laws that seek to regulate face recognition do not preempt state and local bans. Given the concerns outlined above, one thing is clear: policymakers must act to protect the public from this dangerous technology now.

³⁷ See, e.g., Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* (2018), available at <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>.

³⁸ A false positive occurs when a person is incorrectly matched to a photo in the database when it is not actually them. A false negative occurs when the system incorrectly fails to match a person to their photo in the database.

³⁹ Patrick Grother, Mei Ngan, and Kayee Hanaoka, "NISTIR 8280: Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects," National Institute of Standards and Technology (December 2019), <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>.

⁴⁰ *Id.* at 40.

⁴¹ Clare Garvie & Jameson Spivack, *A Taxonomy of Legislative Approaches to Face Recognition in the United States* (Sept. 2, 2020), available at <https://ainowinstitute.org/regulatingbiometrics-spivack-garvie.pdf>.

Signatories:

Access Now
 Action Center on Race and the Economy
 American Civil Liberties Union
 Amnesty International USA
 Asian Americans Advancing Justice – AAJC
 Athena
 Brennan Center for Justice
 Center for Democracy & Technology
 Center on Privacy & Technology at Georgetown Law
 Center on Race, Inequality, and the Law at NYU Law
 Color of Change
 Defending Rights & Dissent
 Demand Progress Education Fund
 Demos
 Electronic Frontier Foundation (EFF)
 Electronic Privacy Information Center (EPIC)
 Fight for the Future
 Free Press
 Government Information Watch
 Innocence Project
 Just Futures Law
 Lawyers' Committee for Civil Rights Under Law
 The Leadership Conference Education Fund
 The Leadership Conference on Civil and Human Rights
 Legal Aid Society of New York City
 Media Alliance
 MediaJustice
 Mijente
 NAACP Legal Defense and Educational Fund, Inc.
 National Association of Criminal Defense Lawyers
 National Coalition Against Censorship
 National Hispanic Media Coalition
 New America's Open Technology Institute
 Oakland Privacy
 OCA – Asian Pacific American Advocates
 Open MIC (Open Media and Information Companies Initiative)
 Project on Government Oversight
 Public Citizen
 Restore The Fourth
 S.T.O.P. – The Surveillance Technology Oversight Project
 Upturn
 X-Lab



July 13, 2021

The Honorable Sheila Jackson Lee
Chairwoman
House Committee on Judiciary, Subcommittee
on Crime, Terrorism, and Homeland Security
6340 Neil House Office Building
Washington, DC 20515

The Honorable Andy Biggs
Ranking Member
House Committee on Oversight and Reform
on Crime, Terrorism, and Homeland Security
6340 Neil House Office Building
Washington, DC 20515

Dear Chairwoman Jackson Lee and Ranking Member Biggs:

On behalf of the Security Industry Association (SIA), thank you for holding today's hearing focused on law enforcement's use of facial recognition technology. SIA represents over 1,100 innovative companies that provide safety and security technology solutions essential to public safety and the protection of lives, property, information, and critical infrastructure. SIA members include companies that provide advanced security solutions to the U.S. Department of Homeland Security, the U.S. Department of Justice, the U.S. Department of Defense, and their component agencies.

SIA believes all technology products, including facial recognition, must only be used for purposes that are clearly defined, lawful, ethical, and non-discriminatory. SIA has taken steps to support related policies by: 1) developing and publishing [policy principles](#) that will help ensure facial recognition is used in a responsible and effective manner; 2) providing [specific policy recommendations](#) to the Biden Administration and Congress that address concerns about facial recognition technology while maintaining U.S. leadership in future development; and 3) providing information regarding the benefits of many technology applications, including [success stories](#) from over a decade of use in U.S. law enforcement investigations, such as how facial recognition technology was used to help rescue a child sex trafficking victim in California, identify a serial armed robber in Indiana, help verify the identity of a man in Pennsylvania accused of sexually assaulting a 15 year-old girl, and help identify an alleged rapist in New York City, to name just a few of many thousands.

Responsible implementation and use of facial recognition technology should include appropriate transparency and accountability measures, stakeholder education, and addressing privacy considerations and civil liberties protections. The [June 2021 GAO report](#) entitled, *Facial Recognition: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, provides an in-depth review of how Federal agencies that employ law enforcement officers use facial recognition technology to assist in criminal investigations and recommends implementing additional internal mechanisms and policies that ensure Federal personnel track what non-federal systems – e.g., state, local, tribal, or territorial entities – are used by their employees. Agencies should have full visibility into the technologies relied upon for criminal investigations and have measures in place to ensure personnel are using facial recognition systems for defined and authorized purposes. Furthermore, GAO recommends that Federal agencies assess certain risks of using these systems, including privacy and accuracy-related risks, so agencies are better positioned to mitigate potential risks to themselves and the public. [SIA strongly supports measures](#)

that increase transparency across the Federal government with respect to use of facial recognition technology and continue to build public trust that it is being used effectively and appropriately.

At the request from members of the House Science, Space & Technology committee, GAO released a relevant [technology assessment](#) in July 2021 entitled, *Forensic Technology: Algorithms Strengthen Forensic Analysis, but Several Factors Can Affect Outcomes*. GAO provided law enforcement agencies with another series of policy recommendations to improve its use of forensic technologies and algorithms – including facial recognition algorithms. After conducting extensive research, GAO did not recommend a ban or moratorium on the use of facial recognition algorithms. Rather, GAO found that “facial recognition algorithms help analysts extract digital details from an image and compare them to images in a database. These algorithms can search large databases faster and can be more accurate than analysts.” Within the assessment, GAO acknowledged the value of the technology and the opportunity to address various challenges related to law enforcement’s use of facial recognition algorithms by recommending robust policy options to: 1) increase personnel training that could reduce risks created by human error, address cognitive biases and improve objectivity in analyses, and provide analyst certification processes; 2) apply flexible, consensus-driven standards for testing and performance of facial recognition algorithms; and 3) improve public access to test data that is constructed in a legible format that increases transparency and builds public trust among communities. SIA recognizes that additional work and innovation is required in order to fully develop related policy proposals, but our industry is encouraged by GAO’s constructive recommendations.

SIA and our members stand ready to contribute to a constructive dialogue surrounding facial recognition technology. Please let us know if there is any way we can assist you as you continue to examine these issues.

Sincerely,



Don Erickson
CEO – Security Industry Association

Cc: Members of the House Judiciary Committee

For more information, please contact Joe Hoellerer, SIA Senior Manager of Government Relations, at jhoellerer@securityindustry.org



WRITTEN STATEMENT of TAWANA PETTY
National Organizing Director, Data for Black Lives

Before the
Subcommittee on Crime, Terrorism, and Homeland Security
House Committee on the Judiciary
Hearing on: Facial Recognition Technology: Examining Its Use by Law Enforcement
Tuesday, July 10, 2021

Dear Chair, Vice-Chair, Ranking Member and Members:

My name is Tawana Petty. I am a lifelong resident of the City of Detroit. I serve as the National Organizing Director at Data for Black Lives, a convening member of the Detroit Digital Justice Coalition and a non-resident fellow of the Digital Civil Society Lab at the Stanford Center on Philanthropy and Civil Society.

Data for Black Lives is a movement of activists, organizers, and mathematicians committed to the mission of using data science to create concrete and measurable change in the lives of Black people. The Detroit Digital Justice Coalition is comprised of people and organizations in Detroit who believe that communication is a fundamental human right. We attempt to secure this right through activities that are grounded in the [digital justice principles](#) of: access, participation, common ownership, and healthy communities. The Digital Civil Society Lab aims to understand and inform civil society in a digitally dependent world.

I value the use of data for technological innovation and recognize its significance in bettering the lives of millions of people. Whether it's through identifying and responding to community members who lack access to the internet, collecting data to implement tools that support community members with disabilities or chronic illnesses (myself included), or the use of data to understand and engage in the political process -- data is leveraged for technological innovation and the evolution of humankind.



However, at Data for Black Lives we understand that data is too often wielded as an instrument of oppression, reinforcing inequality and perpetuating injustice. As an example, redlining was a data-driven enterprise that resulted in the systematic exclusion of Black communities from key financial services. Facial recognition, a form of biometric data, poses a similar, more dangerous threat to our communities, most prominently Black communities.

Prior to the misidentification cases of Robert Williams, Michael Oliver and Nijeer Parks, I stood before Detroit's Board of Police Commissioners and the Detroit City Council to plead the case that misidentification cases were inevitable. I cited the Gender Shades Study by Joy Buolamwini, Timnit Gebru and Deborah Raji and I cited the NIST Study, both of which recognized the discrepancies in how facial recognition sees or does not see darker skin tones. I also cited a study by Georgetown's Center on Privacy and Technology, which pointed to the ways facial recognition was already being manipulated by law enforcement.

I spoke about the feeling residents had of being watched, but not seen. A sense I learned from my research work with Our Data Bodies, a research collective concerned about the ways our communities' digital information is collected, stored, and shared by government and corporations. We rooted our research in marginalized neighborhoods in Charlotte, North Carolina, Detroit, Michigan, and Los Angeles, California. We interviewed approximately 150 residents who consistently expressed for us that they felt that their information was being extracted from them for the benefit of corporations, law enforcement and governmental institutions, but not for their benefit. They indicated that the smallest *mistakes* in their lives, i.e., an inability to afford their water bills, was trailing them and preventing them from upward mobility. They also indicated that they felt targeted by surveillance structures, whether they were a formerly incarcerated resident who had served their time and was trying to get back on their feet, or a person who had been previously evicted from their home but was trying to make a fresh start. The feeling of being targeted but not valued as a human being was consistent across all three cities.

I spoke these concerns before commissioners and city officials for several months on a weekly basis. I spoke about the median household income of Detroiters being under \$31,000 per year, a number sliced nearly in half through job loss, since the pandemic. I spoke about the impact that quality-of-life issues had on quality-of-life crime and provided potential solutions for making a positive impact on the lives of residents, so that we could all begin to feel safer. I pleaded with the civilian oversight body to end the Detroit Police Department's use of facial recognition, because I knew that one day, they would



arrest the wrong the person, or worse, place them in a situation where either them or the officer could lose their life.

Despite my consistent pleas and the testimonials of hundreds of residents, submitted petitions, demonstrations and town halls, the Board of Police Commissioners did not ban facial recognition, but decided to finally put a policy in place to govern it. A policy that was not put in place until the public began to demand a ban. In fact, the public was not aware that facial recognition was being used.

The Detroit Police Department had been using facial recognition for over a year under a standard operating agreement, without a public hearing, and with no oversight from the civilian oversight body. Since the policy has been put in place, we have been made aware of two known misidentification cases involving Detroit Police and a third in New Jersey. We have also been made aware that facial recognition in Detroit is used 100% of the time on Black residents, and despite the fact that the policy is to be used for violent crimes only, it is still being used for non-violent crimes. It is also important to note that under the current policy, the Detroit Police Department is prohibited from tracking residents in real-time. However, the Detroit City Council not only approved an additional \$220,000 to extend the DataWorks Plus facial recognition contract (despite massive protests last year and hundreds of residents attending the hearing in protest), but they also recently approved an additional \$51,000 for BriefCam, which would allow a rapid search of videos across locations.

Detroiters are suffering a great deal of economic disparity. Thousands of residents were overtaxed more than \$600 million dollars leading to massive tax foreclosures, a situation which has not been rectified. Water shutoffs, which community leaders had to fight to end despite Detroiters suffering thousands of deaths during the pandemic - - are on hold until 2022, but still a looming threat to our health and safety. Our infrastructure is crumbling and residents suffered tremendous damage to their homes during the recent flooding, with more flooding on the horizon.

Surveillance is not safety. Massive investment in mass surveillance programs like Project Green Light, which prioritize police presence to private businesses (identified as priority 1) over the safety of residents, while incorporating facial recognition, will not create the type of environment Detroiters deserve. Our movements around our city are being regulated by the thousands of flashing green lights that never go off. If your bedroom is behind one of these lights, you simply don't get a good night sleep. I live under the constant feeling that I am in a perpetual line-up, being monitored everywhere I go. It has had an impact on the businesses I visit, although sometimes I am still forced to patronize establishments that use facial recognition out of necessity. The ubiquitous feeling of being surveilled is



sometimes difficult to describe. One that keeps your shoulders tense with the dread that you might be the next person misidentified and falsely accused of a crime because the face recognition algorithm thinks your driver's license or state id matches one of the images captured at a crime scene.

If research and history is any indication, the three known misidentification cases are just the tip of the iceberg. It is my fear that we will look up 40 years from now, if we do nothing, and have to exonerate people (some posthumously) who spent decades in jail because they were arrested by a faulty, racially biased algorithm. Or worse, we may never find out who they are.

If we fail to act, we will continue to see cities like Detroit fall further and further into the realm of a China-like social credit systems, surrounded by surveillance cameras, real-time crime centers, drones and facial recognition, funneling more and more Black residents unjustly into the criminal justice system. We have already learned a great deal since the rise of mass incarceration. Facial recognition has the potential increase the incarceration disparity to a degree that we won't even be able to quantify.

It's time we rid ourselves of this technology before the harm is irreversible. We have a long way to go in increasing racial equity within our police departments. We should not be exacerbating existing inequity by turning over policing to artificial intelligence.

I have spoken mostly from my perspective as a Detroit, but I do so with the understanding that if racial inequity succeeds in Detroit, it will most likely be packaged and rolled out across Black and Brown communities across the United States.

Please consider ending police use of facial recognition technology. Our data, biometric or otherwise, should not be weaponized against us.

Sincerely,

A handwritten signature in black ink, appearing to read "Tawana Petty".

Tawana Petty
National Organizing Director,
Data for Black Lives



EFF Statement for the Record on Hearing: Facial Recognition Technology: Examining Its Use by Law Enforcement

To: Members, U.S. House Committee on the Judiciary, Subcommittee on Crime

From: The Electronic Frontier Foundation

Date: July 13, 2020

RE: Facial Recognition Technology: Examining Its Use by Law Enforcement

EFF Statement for the Record

Face surveillance is increasingly an all-encompassing tool for government to track where we are, what we are doing, and who we are with, regardless of whether we're suspected of a crime or not. Many proponents of the technology argue that there is no reasonable expectation of privacy when we spend time in public, and that if we have nothing to hide, we have nothing to fear. However, in his majority opinion in the watershed *Carpenter v. United States* (2018)¹, Supreme Court Chief Justice John Roberts wrote: "A person does not surrender all Fourth Amendment protection by venturing in the public sphere."

Advocates for facial recognition and face analysis technologies often present these systems as a "silver bullet," not just for law enforcement, but also to identify customers, to authorize entry into public and private spaces, and even to track people's moods and emotions. However, these technologies frequently reach erroneous conclusions, especially concerning people of color and women,² leading to false arrests of at least three black men.³ Many of the current means for measuring accuracy fail to take account of operational realities and limitations when these systems are used in real-world situations.

Moreover, these technologies present serious challenges to privacy, free expression, and due process. They turn our movements, and thus our lives, into open books for government scrutiny. They also discourage people from exercising their First Amendment rights. The ability for law enforcement to pan over a crowd at a protest, and using face recognition, attempt to identify everyone in attendance, is a severe threat to free political expression and makes people vulnerable to retribution and reprisals. Just last week, the *South Florida Sun-Sentinel* broke the news that three Florida police departments have used face recognition to identify BLM protesters.⁴

¹ *Carpenter v United States*, 585 U.S. ____ (2018)

² Joy Boulamwini, The Algorithmic Justice League, <https://www.ajl.org/>

³ Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. Times (December 29, 2020), <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>

⁴ Joanne Cavanaugh Simpson, Marc Freeman, *South Florida police quietly ran facial recognition scans to identify peaceful protesters. Is that legal?*, South Florida Sun Sentinel, (June 26, 2021), <https://www.sun-sentinel.com/local/broward/fl-ne-facial-recognition-protests-20210626-7sll5uuaqfbaba32rndlv3xwxi-htmlstory.html>



Excessive secrecy surrounding face surveillance also violates the due process rights of people accused of crimes. For one example, Willie Allen Lynch is currently serving an eight-year prison sentence after a facial recognition system suggested him as a likely match of a suspect.⁵ Prosecutors in the case didn't disclose information about how the algorithm worked, that it produced other matches that were never considered, or why Lynch's photo was targeted as the best match.⁶

Lynch didn't learn that he had been identified by a facial recognition algorithm until just days before his final pretrial hearing, although prosecutors had known for months. The crime analyst who operated the system did not know how the algorithm functioned, and neither did the detective who accepted the analyst's conclusion that Lynch's face was a match. The analyst said the first-listed photo in the search results is not necessarily the best match—it could be one further down the list. A prosecutor doubted the system was reliable enough to meet standards used by courts to assess the credibility of scientific testimony and whether it should be used at trial. Lynch asked for the other matches produced by the technology—but the court refused.

If a human witness who identified Lynch in a line-up said others in the line-up also looked like the criminal, the state would have had to disclose that information, and Lynch could have investigated those alternate leads. The same principle should have required the state to disclose other people the algorithm produced as matches, and also information about how the algorithm functions.

When defendants are facing lengthy prison sentences or even the death penalty, tight controls on the use of facial recognition are crucial. Defendants have a due process right to information about the algorithms used and search results. Of course, current violations of the rights of the accused are just one more reason why government must not use face surveillance at all.

Law enforcement agencies have also proven they cannot be trusted with this technology. While often described as nothing more than an investigatory lead, police have arrested people whose names were produced by face recognition technology without corroborating evidence or follow-up investigation, leading to arrests of innocent people.⁷

Because of these well documented problems and disparate impacts, cities and states across the country have banned government use of face surveillance technology, and many more are weighing proposals to

⁵ Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. Times (January 12, 2020), <https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html>

⁶ Amici Curiae Brief of American Civil Liberties Union, American Civil Liberties Union of Florida, Electronic Frontier Foundation, Georgetown Law's Center on Privacy and Technology, and Innocence Project in support of Petitioner, *Lynch v. Florida*, Amicus Brief Filing # 86179154 (2019), <https://www.eff.org/document/lynch-v-florida-amicus-brief>

⁷ American Civil Liberties Union, *Michigan Father Sues Detroit Police Department for Wrongful Arrest Based on Faulty Facial Recognition Technology* (April 13, 2021), <https://www.aclu.org/press-releases/michigan-father-sues-detroit-police-department-wrongful-arrest-based-faulty-facial>



do so. From Boston⁸ to San Francisco⁹, New Orleans¹⁰ to Minneapolis¹¹, elected officials and activists know that face surveillance gives police the power to track us wherever we go, disproportionately impacts people of color¹², turns us all into perpetual suspects, increases the likelihood of being falsely arrested¹³, and chills people's willingness to participate in first amendment protected activities.

Police and other government use of this technology cannot be responsibly regulated. Face surveillance in the hands of the government is a fundamentally harmful technology, even under strict regulations or if the technology was 100% accurate and disclosed. The use of face surveillance by the federal government should be banned, and certain federal funds should be withheld from local and state governments that use the technology.

⁸ Matthew Guariglia, *Victory! Boston Bans Government Use of Face Surveillance*, The Electronic Frontier Foundation (June 24, 2020), <https://www.eff.org/deeplinks/2020/06/victory-boston-bans-government-use-face-surveillance>

⁹ Nathan Sheard, *San Francisco Takes a Historic Step Forward in the Fight for Privacy*, Electronic Frontier Foundation (May 14, 2019), <https://www.eff.org/deeplinks/2019/05/san-francisco-takes-historic-step-forward-fight-privacy>

¹⁰ Michael Isaac Stein, *New Orleans City Council bans facial recognition, predictive policing and other surveillance tech*, The Lens (December 18, 2020) <https://thelensnola.org/2020/12/18/new-orleans-city-council-approves-ban-on-facial-recognition-predictive-policing-and-other-surveillance-tech>

¹¹ Kim Lyons, *Minneapolis prohibits use of facial recognition software by its police department*, The Verge (February 13, 2021), <https://www.theverge.com/2021/2/13/22281523/minneapolis-prohibits-facial-recognition-software-police-privacy>

¹² Alex Najibi, *Racial Discrimination in Facial Recognition Technology*, Harvard University (October 24, 2020), <https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology>

¹³ Drew Harwell, *Wrongfully arrested man sues Detroit police over false facial recognition match*, Washington Post (April 13, 2021), <https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit>



Thank you for the opportunity to submit a statement to the House Judiciary Committee Subcommittee on Crime, Terrorism, and Homeland Security regarding its hearing, “Facial Recognition Technology: Examining Its Use by Law Enforcement.”

The Project On Government Oversight (POGO) is a nonpartisan independent watchdog that investigates and exposes waste, corruption, abuse of power, and when the government fails to serve the public or silences those who report wrongdoing. The Constitution Project at POGO strives to protect constitutional rights and principles, including guarding against improper and overbroad surveillance such as unchecked face recognition. In 2019, the Constitution Project convened a task force of expert stakeholders including academics, tech experts, civil rights and civil liberties advocates, and law enforcement officials to examine the impact of face recognition surveillance.¹ It concluded that any law enforcement use of face recognition should be subject to strong limits, and provided a set of policy recommendations.

Face recognition surveillance poses two distinct but equally important dangers: It can be immensely harmful when it does not function properly, and it can also be immensely harmful when it does. Face recognition misidentifications can lead to improper targeting, needless police action, and wrongful arrests. Innocent individuals could face jail time or be pressured to take a plea deal, all without knowing charges were based upon a poor face recognition match. But making face recognition more accurate will not alleviate the danger it poses to civil rights and civil liberties. Absent strong limits, face recognition opens the doors to pervasive surveillance and abuse, and it allows the government to warp discretion into a tool for malicious and selective targeting.

Correcting Common Misconceptions about Face Recognition Surveillance

As lawmakers consider what safeguards to place on face recognition surveillance, it is important to recognize common misconceptions about law enforcement use of the technology and the damage it causes. This section corrects four key misconceptions about face recognition and explains why the realities about it require urgent action by Congress.

Face recognition does not work in a monolithic way; in reality, its ability to function—and the limits of its functionality—are highly situational.

Face recognition is frequently portrayed in crime dramas—and more disturbingly, by vendors selling the technology—as a technology that can be applied to photos in any situation, with consistently accurate results. In reality, face recognition’s ability to deliver reliable matches depends upon a range of factors.

¹ Task Force on Facial Recognition Surveillance, Project On Government Oversight, *Facing the Future of Surveillance* (March 4, 2019), <https://www.pogo.org/report/2019/03/facing-thee-future-of-surveillance/>.

The quality of face recognition algorithms can vary significantly. Notably, many algorithms misidentify women and people of color at a higher rate than other people. Studies by the National Institute of Standards and Technology; the Massachusetts Institute of Technology, Microsoft, and AI Now Institute researchers; the American Civil Liberties Union; and an FBI expert all concluded that face recognition systems misidentify women and people of color more frequently.² Most recently, the National Institute of Standards and Technology found that some systems were 100 times more likely to misidentify people of East Asian and African descent than white people.³ Failure to recognize the significance of this problem—and account for it in selection and review of software, training, and auditing—will undermine investigations and seriously harm civil rights.

Image quality can also significantly impact accuracy of matches. Sets of reference images—databases containing previously identified faces—in face recognition systems are typically high-resolution photos of a person directly facing a camera at close range, such as for a mug shot photo. But probe images—from which law enforcement seeks to identify individuals—are derived from a wide range of situations, which creates the potential for low image quality and erroneous results.

Bad lighting, indirect angles, distance, poor camera quality, and low image resolution all make misidentifications more likely.⁴ These poor image conditions are more common when photos and videos are taken in public, such as with a CCTV camera. But these low-quality images often serve as probe images for face recognition scans, without due consideration for their diminished utility.⁵

Even when using more effective software and higher quality images, system settings can make face recognition matches prone to misidentification. For example, the way law enforcement sets confidence thresholds—a metric used to compare which proposed matches within a system are more likely to be accurate—can undermine reliability of results. The lower the confidence threshold, the more likely the “match” is actually a false positive. So, if law enforcement

² Patrick Grother, Mei Ngan, Kayee Hanaoka, National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTIR 8280 (December 19, 2019), 2, <https://doi.org/10.6028/NIST.IR.8280>; Joy Buolamwini and Timnit Gebru, “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,” *Proceedings of Machine Learning Research*, vol. 81 (2018), <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>; Joy Buolamwini and Inioluwa Deborah Raji, “Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products,” *AIES ’19: Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society* (2019), <https://www.media.mit.edu/publications/actionable-auditing-investigating-the-impact-of-publicly-naming-biased-performance-results-of-commercial-ai-products/>; Jacob Snow, “Amazon’s Face Recognition Falsely Matched 28 Members of Congress With Mugshots,” American Civil Liberties Union, July 26, 2018, <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>; Brendan Klare et al., “Face Recognition Performance: Role of Demographic Information,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6 (December 2012), <http://openbiometrics.org/publications/klare2012demographics.pdf>.

³ Grother, Ngan, Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, 2 [see note 2].

⁴ Task Force on Facial Recognition Surveillance, *Facing the Future of Surveillance*, Sec. II [see note 1].

⁵ “CCTV feeds facial recognition systems for law enforcement,” *Biometric Technology Today*, vol. 2015, no. 4 (April 2015): 3, <https://www.sciencedirect.com/science/article/abs/pii/S0969476515300539>.

entities set face recognition systems to always return potential matches—no matter how low confidence the threshold—they will receive untrustworthy data. Troublingly, some law enforcement entities do just that.⁶

For example, one police department designed its face recognition system so that for field use it “dropped the search-confidence percentages and designed the system to return five results, every time,” meaning results would come back as top possible matches even if they were unreliable, introducing the likelihood that officers would receive untrustworthy information amid encounters with individuals.⁷

Disturbingly, the vendors that sell face recognition software often exaggerate how broadly the technology functions, thereby encouraging irresponsible law enforcement use that will lead to misidentifications.

One major vendor boasts in marketing materials that “facial recognition gives officers the power to instantly identify suspects. . . . Officers can simply use their mobile phones to snap a photograph of a suspect from a safe distance. If that individual is in their database, it can then positively identify that person in seconds with a high degree of accuracy.”⁸ This is an inflated characterization given the limits that lighting and angle would impose in such a situation. Other vendors claim face recognition would offer a positive identification—rather than provide a set of possible but uncertain matches—but that claim is at odds with how most responsibly designed face recognition systems operate in practice.⁹

Clearview AI’s pitches to law enforcement—obtained through public records requests by *BuzzFeed*—are shockingly boastful. The company claims to have “the most accurate facial identification software worldwide” and to consistently produce accurate results “in less than five seconds.” The company even goes so far as to tell law enforcement that using its software will make them “realize you were the crazy one” for not believing face recognition would perform

⁶ Jim Trainum, “Facial Recognition Surveillance Doesn’t Necessarily Make You Safer,” Project On Government Oversight, July 22, 2019, <https://www.pogo.org/analysis/2019/07/facial-recognition-surveillance-doesnt-necessarily-make-you-safer/>; According to then-FBI Deputy Assistant Director Kimberly Del Greco, its system is set up so that it “returns a gallery of ‘candidate’ photos [reference photos] of 2-50 individuals (the default is 20).” *Facial Recognition Technology (Part II): Ensuring Transparency in Government Use: Hearing before the House Committee on Oversight*, 116th Cong. (June 4, 2019) (statement by Kimberly Del Greco, Deputy Assistant Director, FBI Criminal Justice Information Services Division), <https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use>.

⁷ Drew Harwell, “Oregon became a testing ground for Amazon’s facial recognition policing. But what if Rekognition gets it wrong?” *Washington Post*, April 30, 2019, <https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/>.

⁸ “For Law Enforcement, The Cost of a False Arrest is More Than Just Bad Press,” FaceFirst, October 20, 2017, <https://www.facefirst.com/blog/law-enforcement-cost-false-arrest-far-just-bad-press/>.

⁹ Cognitec states that its software can be used for “fast identification of suspects and efficient crime investigations.” Cognitec, “Applications: Law enforcement,” <https://www.cognitec.com/law-enforcement.html> (accessed July 9, 2021); As of August 2019, DataWorks Plus promised law enforcement “reliable identification through facial recognition technology” and that its software “uses facial recognition technology to positively match photos of an individual by identifying key characteristics of the facial image” with capabilities such as “discovering a person’s identity during investigations.” DataWorks Plus, “Facial Recognition Technology & Case Management,” <http://web.archive.org/web/20190811221236/http://www.dataworksplus.com/80/faceplus.html>.

the same as it does in outlandish TV depictions like “NCIS, CSI, Blue Bloods.”¹⁰ An FAQ the company provided to law enforcement claims, “a photo should work even if the suspect grows a beard, wears glasses, or appears in bad lighting,” then adds, “you will almost never get a false positive. You will either get a correct match or no result.”¹¹ This is a false and incredibly dangerous claim. If law enforcement takes it as true, they may be inclined to put immense weight on *any* face recognition match they receive through Clearview AI software.

And at the same time Amazon publicly stated law enforcement clients should set the company’s face recognition software to only return matches based on a 99% confidence threshold, it was advising at least one department to deploy a top-five-match system that would always return results, even if possible matches were well below that 99% threshold.¹² This augments the risk that misidentifications will be presented to law enforcement as matches.

In the absence of safeguards to address this range of misidentification risks, face recognition will continue to provoke errors, harm innocent individuals, and exacerbate inequalities in how different communities are policed.

Face recognition is not a risk-free tool if law enforcement just uses it for leads; face recognition still can, and does, mislead law enforcement.

It is important to resist the temptation to shrug off the risks of misidentification based on law enforcement claims that face recognition is just used for leads, rather than as the backbone of a prosecution.¹³ Using untrustworthy information as the foundation of investigations is always dangerous, regardless of whether that information is introduced in court.

The simple fact is, unreliable investigative tools and techniques—even if just used for leads and taken alongside other potentially exonerating evidence—can lead to the arrest of innocent individuals, a problem we have seen again and again with flawed technologies ranging from

¹⁰ Jake Laperruque, “Face Recognition Is Far from the Sci-Fi Super-Tool Its Sellers Claim,” Project On Government Oversight, April 16, 2021, <https://www.pogo.org/analysis/2021/04/face-recognition-is-far-from-the-sci-fi-super-tool-its-sellers-claim/>.

¹¹ “Clearview FAQ,” Clearview, https://s3.documentcloud.org/documents/20531944/north-miami-fl-clearview_faq.pdf.

¹² Jake Laperruque, “About-Face: Examining Amazon’s Shifting Story on Facial Recognition Accuracy,” Project On Government Oversight, April 10, 2019, <https://www.pogo.org/analysis/2019/04/about-face-examining-amazon-shifting-story-on-facial-recognition-accuracy>.

¹³ For example, during a 2020 congressional hearing, FBI Director Christopher Wray responded to inquiries on face recognition by stating “We use it for lead value. ... We don’t use facial recognition as a basis to arrest or convict someone.” *Oversight of the Federal Bureau of Investigation: Hearing before the House Judiciary Committee*, 116th Cong. (February 5, 2020), 4:53:28, <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=2780>.

outdated forensics¹⁴ to unreliable polygraph tests.¹⁵ If standard law enforcement policy was to base investigations on smudged fingerprints or contaminated DNA samples, it would be of little comfort that this tainted evidence was just used for leads.

There are already at least three documented cases in which individuals have been improperly arrested based on face recognition misidentifications.¹⁶ It is unlikely that Robert Williams, Michael Oliver, and Nijeer Parks are the only individuals who have been wrongfully arrested because of such errors. According to a 2020 *New York Times* investigation of face recognition systems in Florida, “Although officials said investigators could not rely on face recognition results to make an arrest, documents suggested that on occasion officers gathered no other evidence.”¹⁷ Because face recognition is frequently hidden from defendants,¹⁸ there are likely more instances where face recognition led to the arrest of innocent individuals—some of whom may have felt pressured to accept a plea bargain—that we are unaware of.

Individuals could also be charged in part based on how a match produced by a face recognition system affects the direction of an investigation early on, especially when having a match promotes confirmation bias or sloppy follow-up. For example, in one incident, New York City Police Department officers allegedly took a single possible face recognition match, and then texted a witness, “Is this the guy...?” along with the photo, rather than following proper procedure to use a photo array.¹⁹

Even without leading to improper arrests, face recognition misidentifications can cause serious harm. Being targeted in an investigation can also be disruptive and potentially traumatic, and can endanger individuals even if charges or a conviction never follow.

By holding up the notion that *face recognition is just used for leads* as a virtue, law enforcement actually places this technology in a limbo where its “results still can play a significant role in investigations, though, without the judicial scrutiny applied to more

¹⁴ President’s Council of Advisors on Science and Technology, *Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods* (September 2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf.

¹⁵ Joseph Stromberg, “Lie detectors: Why they don’t work, and why police use them anyway,” *Vox*, December 15, 2014, <https://www.vox.com/2014/8/14/5999119/polygraphs-lie-detectors-do-they-work>.

¹⁶ Kashmir Hill, “Wrongfully Accused By An Algorithm,” *New York Times*, June 24, 2020, <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>; K. Holt, “Facial recognition linked to a second wrongful arrest by Detroit police,” *Engadget*, July 10, 2020, <https://www.engadget.com/facial-recognition-false-match-wrongful-arrest-224053761.html>; Kashmir Hill, “Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match,” *New York Times*, December 29, 2020, <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>.

¹⁷ Jennifer Valentino-DeVries, “How the Police Use Facial Recognition, and Where It Falls Short,” *New York Times*, January 12, 2020, <https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html>.

¹⁸ In some jurisdictions, law enforcement uses facial recognition thousands of times per month, but defendants almost never receive notice of its use in investigations. Valentino-DeVries, “How the Police Use Facial Recognition, and Where It Falls Short” [see note 17].

¹⁹ Clare Garvie, “Garbage In, Garbage Out: Face Recognition on Flawed Data,” Georgetown Law Center on Privacy & Technology, May 16, 2019, <https://www.flawedfacedata.com/>.

proven forensic technologies.”²⁰ It is vital that better safeguards be put into place to prevent improper reliance on this technology, and to ensure that defendants are not deprived of their right to review potentially exculpatory evidence.

The risk that face recognition surveillance will be abused is not hypothetical; the technology has already been abused to target and hamper First Amendment-protected activities.

Face recognition has already been misused to identify peaceful protesters and to facilitate selective prosecution against protesters.

According to a *South Florida Sun Sentinel* investigation, in 2020, law enforcement repeatedly used face recognition to identify and catalog peaceful protesters. Fort Lauderdale police ran numerous face recognition searches to identify people who might be a “possible protest organizer” or an “associate of protest organizer” at a Juneteenth event to promote defunding the police. Boca Raton police also ran face recognition scans on half a dozen occasions throughout May 2020 targeting protesters during peaceful events. And the Broward Sheriff’s Office ran nearly 20 face recognition searches during this same time period for the purpose of “intelligence” collection, rather than to investigate any criminal offense.²¹

Face recognition has been abused for selective targeting, with law enforcement using the technology to rapidly scan protests for individuals with active bench warrants for unrelated offenses. Several years ago, Baltimore police used face recognition amid protests to find individuals with “outstanding warrants and arrest[ed] them directly from the crowd,” in a selective effort that appeared to be aimed at disrupting, punishing, and discouraging demonstrators from protesting.²²

Absent strong rules, these problems will continue to occur. Face recognition could be used to identify and catalog every attendee at a religious service or political rally, akin to a hyper-powered version of the “mosque crawlers” the New York Police Department deployed for its surveillance of Muslim Americans,²³ or the plants and informants the FBI used to spy on activists as part of COINTELPRO.²⁴ Face recognition could catalog who goes to a health clinic,

²⁰ Valentino-DeVries, “How the Police Use Facial Recognition, and Where It Falls Short” [see note 17].

²¹ Joanne Cavanaugh Simpson and Marc Freeman, “South Florida police quietly ran facial recognition scans to identify peaceful protesters. Is that legal?” *South Florida Sun Sentinel*, June 26, 2021, <https://www.sun-sentinel.com/local/broward/fl-ne-facial-recognition-protests-20210626-7sl15uuagfbaba32rmdlv3xwxi-htmlstory.html>.

²² Kevin Rector and Alison Knezevich, “Social media companies rescind access to Geofeedia, which fed information to police during 2015 unrest,” *Baltimore Sun*, October 11, 2016, <https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html>.

²³ Research found that the NYPD Muslim surveillance program resulted in “a striking self-censorship of political speech and activism. Conversations relating to foreign policy, civil rights and activism are all deemed off-limits” and expression of religious identity was also severely chilled as “parents discourage their children from being active in Muslim student groups, protests, or other activism, believing that these activities would threaten to expose them to government scrutiny.” Diala Shamas and Nermeen Arastu, *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, (2013), 4, <https://www.law.cuny.edu/vp-content/uploads/page-assets/academics/clinics/immigration/clear/Mapping-Muslims.pdf>.

²⁴ “FBI Records: The Vault: COINTELPRO,” Federal Bureau of Investigation, <https://vault.fbi.gov/cointel-pro> (accessed July 9, 2021).

substance abuse treatment center, or union meeting. These kinds of sensitive data about people's lives could be stockpiled and used for an immense array of future government activities, ranging from profiling, to selective law enforcement investigations, to evaluations for civil service employment opportunities. And even absent such malicious actions, research has shown that surveillance does in fact chill participation in basic activities, especially when directed at sensitive activities and groups vulnerable to persecution.

The dangers face recognition pose cannot be solved by just restricting use of the most egregious companies and error-prone algorithms; even the most well-designed systems create danger.

When crafting safeguards against face recognition surveillance, lawmakers should not limit their focus just to egregious situations. As the problems described above show, even well-designed systems can cause serious problems.

One face recognition vendor that has garnered significant attention is Clearview AI. Unlike other face recognition systems, Clearview AI builds its reference photo database by scraping billions of photos from social media sites.²⁵ This practice violates the terms of use for the websites hosting the photos and, more importantly, violates the consent and expectations of privacy of users who place images on their account with the promise that they will not be grabbed en masse and misused. Countering this tactic of mass scraping for biometric scanning may require specific legislative rules.²⁶

However, even if law enforcement were totally cut off from using Clearview AI, the general dangers that face recognition surveillance creates would remain. Face recognition systems built on reference photo databases of mugshots or driver's license photos, for instance, can still produce misidentifications for a variety of reasons, and cause serious harms when law enforcement relies on those misidentifications. And face recognition systems built on those same databases can be abused to catalog sensitive activity.

Additionally, while the propensity of many face recognition systems to misidentify people of color at higher rates should be a top priority for lawmakers to address, it is only one of many dangers misidentification poses. Even if systems improved to the point of eliminating algorithmic bias, risks of error will still persist. Because misidentification is often due to poor image quality, even the most reliable systems will remain vulnerable to error. And as long as inequalities exist across our criminal justice system, we can expect the harms of face recognition misidentification to continue to be disproportionately borne by people of color.

Priorities for Lawmakers in Responding to Face Recognition Surveillance

The need for lawmakers to impose strong limits on face recognition is urgent. In the absence of safeguards, roughly half of all adults in the United States already have pre-identified photos

²⁵ Jake Laperruque, "Danger Isn't Just from Government Abuse: Face Recognition in the Hands of Stalkers, Harassers, and Vigilantes," Project On Government Oversight, June 10, 2021, <https://www.pogo.org/analysis/2021/06/danger-isnt-just-from-government-abuse/>.

²⁶ Laperruque, "Danger Isn't Just from Government Abuse" [see note 25].

in databases used for law enforcement face recognition searches, and at least a quarter of the nation's state or local police departments possess the ability to run face recognition searches either directly or via a partnering agency.²⁷ Meanwhile, even more pervasive face recognition systems are being implemented. Numerous cities have developed plans or implemented pilot programs for untargeted face recognition which scan every person within a crowd who passes by the frame of a camera and provide an alert if anyone scanned is identified as a match against preexisting watchlists.²⁸

We are beginning to see significant action to limit face recognition: Over a dozen cities have banned law enforcement use of the technology,²⁹ and multiple states have recently passed laws that require court approval before law enforcement can run face recognition scans and that limit its use to investigating violent felonies.³⁰ But for the vast majority of Americans, face recognition can still be deployed against them absent any rules or safeguards.

The most straightforward solution at this time would be to press pause on face recognition surveillance, enacting a national moratorium on its use, as the Facial Recognition and Biometric Technology Moratorium Act would do.³¹

If Congress does not pursue a full moratorium, there are still safeguards that can limit the dangers face recognition surveillance poses. Preventing irresponsible use of face recognition and reliance on misidentifications necessitates transparency requirements, testing and accuracy standards, rules for training and use, limits on how much weight investigators place on matches, and disclosure to defendants. Guarding against abuse and dragnet collection of sensitive information requires meaningful rules for independent authorization—such as a warrant requirement—and limiting use to investigating serious offenses. The Constitution Project's task force report on face recognition examines many of these policies in detail.³²

Finally, it is vital that any action Congress takes does not preempt restrictions on face recognition passed at the state and municipal level. Many communities have already made clear that they want law enforcement use of face recognition to be fully prohibited, and their preference should be respected. Other cities and states may wish to implement additional restrictions on face recognition that Congress does not consider; this could be especially valuable given rapid developments in how the technology is used. Federal legislation on face recognition can only aid civil rights and civil liberties if it makes clear that separate limits at the state and local level will not be overridden.

²⁷ Clare Garvie, Alvaro Bedoya, Jonathan Frankle, Georgetown Law Center on Privacy & Technology, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (October 18, 2016), 8, 25, <https://www.perpetuallineup.org/>.

²⁸ Clare Garvie and Laura Moy, Georgetown Law Center on Privacy & Technology, *America Under Watch: Face Surveillance in the United States*, (May 16, 2019), <https://www.americaunderwatch.com/>.

²⁹ Shannon Flynn, "13 Cities Where Police Are Banned From Using Facial Recognition Tech," *Innovation and Tech Today*, November 18, 2020, <https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/>.

³⁰ S. 2963, 117th Gen. Ct., 2nd Sess. (MA 2020); H.P. 1174, 130th Leg., 1st Spec. Sess. (ME 2021).

³¹ Facial Recognition and Biometric Technology Moratorium Act of 2021, S. 2052, 117th Cong., (2021), <https://www.congress.gov/117/bills/s2052/BILLS-117s2052is.pdf>.

³² Task Force on Facial Recognition Surveillance, *Facing the Future of Surveillance* [see note 1].

Chair NADLER. Thank you.

I yield back.

Ms. JACKSON LEE. Thank you very much.

Mr. Chabot, you are recognized for five minutes.

Mr. CHABOT. Thank you, Madam Chair.

I would like to lead off by thanking our Ranking Member, Mr. Jordan, for allowing me to go in front of him. I have a noon speech that I am supposed to give in my district. It's going to take me awhile to get there, so I really do appreciate him switching spots with me.

In addition to being a Senior Member of the Judiciary Committee for quite a few years, I also serve on the Foreign Affairs Committee, and I'm the Ranking Member and past Chair of the Asia and Pacific Subcommittee, and in that capacity, we, both Republicans and Democrats, on the Committee have been very closely watching, observing, monitoring what the PRC and the Chinese Communist Party is up to there, and the threat that they pose, not only to Americans, but to their own citizens.

It's well known, as was mentioned earlier in the statement of one or two of the Witnesses, that the Chinese Communist Party uses a vast civilian surveillance network to track nearly every movement of every single person there, and there's 1.4 billion people who they are tracking.

So, it's a pretty extensive effort that they have undertaken. For example, they force their citizens to download apps that monitor them. They track social media posts to look for what they consider to be negative content. They stop people at random to check their devices for apps deemed to be dangerous to the state, and they use facial recognition technology, technology similar to what we are discussing here today, to pick individuals up that they are looking for in crowds.

All of this is to build a so-called great firewall between China and the rest of the world, so they can keep their people under control, and to gather personal data on their citizens which can be used to flag and potentially torment the people of China, individuals they believe that are going to be unhelpful to the regime.

So, I would like to ask Ms. Frederick and Mr. Tolman, would you care to comment on the assessment you see relative to China, their use of facial recognition, other technologies, to monitor their citizens and how the CCP is using facial recognition technology to oppress individuals and certainly various groups. The Uyghur community comes to mind because they have obviously been in the news, not nearly enough of late when you consider that a million people are in their gulags.

Are there any lessons that we should learn from this? I'm not, by any stretch of the imagination, suggesting that our government has anything like this in mind; but I would like to hear from those two, if we could.

Ms. FREDERICK. Certainly. Thank you for the question. I will begin, if you don't mind, Mr. Tolman.

So, we should say yes, we have a system in the United States here that matters, sufficient rule-of-law protections, openness and engaged citizenry, a free press, and an independent judiciary that

Act as guardrails for now against the propagation of technology for political ends that are anywhere near like China.

It is important to look to them. As I said before, they are the bleeding edge of using these technologies for internal control and internal stability. They pervade a path for ethnic targeting in the western region of Xinjiang as we talked about, where 1.5 million Uyghurs are imprisoned in reeducation camps often through the use of these facial recognition systems.

It's not just about facial recognition alone. I think the ability to integrate seemingly disparate data sets as they do in Xinjiang, they use something that Human Rights Watch has reverse-engineered. It's called the Integrated Joint Operations Platform, and what they do is they take all this data, they fuse it. It's license plate readers, data doors, these things that pick-up SIM cards, and all kinds of biometrics, iris scans, just all the digital exhausts that we are constantly emitting that people, even in these regions, are constantly emitting. They put them altogether, and they use this information. They use new technology, artificial intelligence—this is one of the first places that they started using it—for political identification of dissidents, of Uyghur minorities.

What I see coming down the pike is the use of DNA genotyping. China is already trying to do this. They are trying to use an individual's DNA to predict what their faces will look like. They are experimenting with voice recognition technologies, and the idea is to combine all this into this digital panopticon and use it for basically an iron hand of digital control. We have the technology right now to do so.

They have visited some of this in Hong Kong, as we have seen the diminishing of freedoms there, how does the democracy die in full view of us, and China is using technology to enact it. We know that Russia is doing the same things when it comes to pro-Navalny protests in January of this year. So, all these things are something to keep in mind. As Paul Mozur from *The New York Times* said, which I think is something that I would leave you with, "what China is trying to do is totalized control." They are trying to link digital reality with physical reality, and that chasm that used to exist is growing closer and closer and closer together. China wants them to be completely interconnected. We have to guard against that here in America.

Mr. CHABOT. Thank you.

Madam Chair, my time is expired. Perhaps Mr. Tolman could respond in writing just so we don't hold the Committee up at this time.

Ms. JACKSON LEE. Thank you very much, Mr. Chabot, for yielding back.

I now recognize the gentlelady from California, Ms. Bass, for five minutes.

Ms. BASS. Thank you, Madam Chair, and let me thank the Ranking Member and our Witnesses for being with us today.

I wanted to know if the Witnesses—and anyone could speak—could distinguish between using facial recognition to investigate versus facial recognition for arrest. Is it more productive to use it that way versus all the complications for arrest?

Also, it's very well-known, and it has been said by numerous panelists and Members, of the challenges of facial recognition with people of color, but I'm not sure, unless I missed it, if anybody said, "Does it work better if it's White men?" How does it perform?

Dr. Alexander, would you like to go?

Dr. ALEXANDER. Well, I will try to respond, to the first part of your question, whether the technology should be utilized with the idea of making an arrest based on the identification itself, can it be used as an investigative tool?

When I think about it as an investigative tool, if that person's image happened to be a match, or similar match and we are working with zero leads in a case, it may prove to be of some value, right? The thing we have to be very careful—and I think someone mentioned it earlier and articulated it far better than I can—that we have to make sure we cognitively don't approach that individual already with our implicit biases in mind that they are the exact person we are looking for. Do you follow what I'm saying, Congresswoman? So, I think we have to be very, very careful with that.

Ideally, to be perfectly honest with you, I was here two years ago under the leadership of another hearing with the late Congressman Elijah Cummings having these same conversations, and I recollect very clearly there was a woman there who was a professor, researcher at MIT who spoke very eloquently around these issues and was able to provide some insight in terms of the depth of this technology and how it does not work to the advantage of people of color and women.

There's an overwhelming amount of evidence—and I think there are those on this panel who can talk further about this—where, in the case of White males, there was the least likely opportunity for misidentification. Certainly, those of color and women, they tend to be more problematic.

Ms. BASS. You said least likely, meaning that it's more accurate with White men?

Dr. ALEXANDER. Yes. It's more accurate with White men. I'm sorry, yes.

Ms. BASS. Maybe someone else could respond to that. I don't know whether it's Mr. Friedman or Ms. Goodwin. What about that in terms of the accuracy and its use as an investigative tool? In the George Floyd Justice in Policing Act, we essentially say there should not be Federal resources in facial recognition.

Mr. Williams, you have your hand raised.

Mr. WILLIAMS. I was just going to say about the question you had previously asked that it was supposed to be used for an investigative tool at that point, and they came and arrested me and didn't even tell me anything. I don't even live in Detroit, and Detroit police came to my house in Farmington Hills, and basically carted me off. Right. So, I don't have a lot to say about that. All I'm saying is that the way that it's used, they are not doing any due diligence at all. That, like the chief said, was shoddy investigative work done and—

Ms. BASS. Actually, excuse me, Mr. Williams, to me you are an example of what I wasn't saying. I

Mr. WILLIAMS. I was talking about when you asked the question.

Ms. BASS. Right. They used it for your arrest—

Mr. WILLIAMS. Right.

Ms. BASS. —which I think it's clear is problematic; but I was referring to use it to investigate, not in real time for an arrest.

Mr. Friedman, do you have anything you want to say in the last few seconds?

Mr. FRIEDMAN. Sure. I think there are things that this body could do regulatorily, and then there are things that it could learn and try to get us to learn. One of the problems we have is that NIST has not tested the kinds of uses that law enforcement is using. What we need—and I'm happy to elaborate, but I don't want to go over time—is the kind of testing that actually reflects what's happening in law enforcement news rather than a set of abstract possibilities for the accuracy and bias.

Ms. BASS. Thank you, Madam Chair.

Ms. JACKSON LEE. Thank you so very much.

Mr. Ranking Member, I'm not going to take up your time, but I am just moved to say that it appears like unreasonable search and seizure under the Fourth Amendment. I will not take up your time, and I'm delighted to recognize Mr. Jordan for five minutes.

Mr. JORDAN. Thank you, Madam Chair.

Let me go over to Mr. Tolman. How often does it happen, how often do we get the wrong person? Where Mr. Williams told his compelling story of how they were just wrong and he was arrested and detained, I think he said for 30 hours—I know the Hueper family, the recent story of the couple in Alaska who were not in the Capitol on January 6, but their door was kicked in. They were put in handcuffs. They were at gunpoint at one point during the interrogation. It was like a four-hour interrogation, and it was all based on facial recognition. So, how often do we get the wrong person?

Mr. TOLMAN. Well, one time would be too many, but certainly, some estimate it as high as 30 percent, but I actually believe it's more than that, Representative Jordan. It's nice to see you again, sir.

Mr. JORDAN. You too.

Mr. TOLMAN. It is, I believe, higher than that. I have represented two individuals, one of whom I'm fairly certain—and it's not—we don't know about the ones that aren't publicized or the ones that aren't coming forward. I have a client who was accused of going inside of the Capitol. He was not in the Capitol. I believe it was facial recognition technology that put him in law enforcement's investigation, and we certainly had to work backwards to show that he was not.

So, I think it's more often than we know because it's not being reported.

Mr. JORDAN. Mr. Lee, do you know? Is there any kind of—Mr. Tolman said 30 percent. Is that—and we know it's a disproportionate impact on African Americans. Do you think it's a higher number than that, or is that probably where that 30 percent of the time this technology gets the wrong person?

Mr. LEE. Ranking Member Jordan, thank you for the question.

We don't know, and that's a part of the problem. These technologies lack the requisite transparency and the requisite oversight for us to even know. Of the cases like Mr. Williams' that we do

know those are terrifying. What about the cases that are maybe on the knife's edge that we don't know about right now? So, we do need more transparency and more oversight, specifically with facial recognition technology and its use by law enforcement.

Mr. JORDAN. Yes, thank you.

I'm going to yield to our Ranking Member, but I'm concerned, in a general sense, that just the overall surveillance State and individual Americans' just fundamental liberties, fundamental rights, but when you add on top of that the fact that it's wrong so often, to me, this is why if we can't come together in a bipartisan fashion as I know we have been trying now for a couple of years, if we can't do that and figure out a way to put restrictions on this, limit this, particularly when you have all these agencies using the technology, they don't even know which technology they're using, and whether it's private or what have you—there's just a host of problems here.

So, I appreciate Chair Jackson Lee having this hearing, and I'm going to yield the remaining two minutes to our Ranking Member, Mr. Biggs.

Mr. BIGGS. I thank the gentleman for yielding.

My question at this time is to you, Ms. Frederick. Peachtree Corners, Georgia, used AI-driven Smart cameras to monitor social distancing, social distancing, and use of mastering COVID-19.

With current technology, what prevents Federal agencies or State and local government from using facial recognition not just to use it for identification, but to track movement and behavior of law-abiding citizens?

Ms. FREDERICK. I fear that's what is coming down the pike, and right now, there are specific transparency measures and lukewarm, I would say, strictures on some of these uses. Ms. Goodwin talked very well about the PIA and the SORN, and JO's recommendations. Those are great start points, but at this point, there are no hard constraints on the expansion of the remit for these cameras. So, the public safety remit, it's huge. It could encompass all sorts of things, and, clearly, certain municipalities are taking advantage of that to interpret public safety as they wish.

So, unless Federal entities are required to really submit those efficacy reports, those transparency reports that don't yet exist in a very rigorous fashion, then I fear many official entities will be allowed to interpret the use of facial recognition, interpret the use of digital surveillance in any way they can.

I will say quickly, when I was at Facebook, the ethos of private companies in shipping these products—and this is the problem with private companies being used by Federal entities you want to ship it. You want to ship it. You deploy these technologies as fast as you can and solve problems in the rollout in later iterations. That ethos is—

Mr. BIGGS. So, Ms. Frederick, thank you for answering that. I need to ask one more question because it deals with—and I want to talk to Professor Laurin really quick. She had her hand raised with regard to the question on investigation versus arrest. What has come to my mind is this notion of tainted photo lineups, tainted identification being used in investigation as predicate for making an arrest.

Did you want to elaborate on that, Professor Laurin?

Ms. LAURIN. Thank you so much for the opportunity, Mr. Ranking Member.

I will say just a bit more, and that's to say that I do think that it's possible in theory to think about a distinction in the use of the technology as an investigative tool versus forming the basis for an arrest or put differently, a facial recognition match by itself forming probable cause, right, to arrest.

I think that from a regulatory standpoint, one needs to take great care in thinking about what strictures need to be put in place to create a meaningful distinction between those two things, right? So, for example, there are a number of agencies that currently say facial recognition itself cannot be the basis for probable cause. Then there are very few, if any, sort of strictures around what further investigation is required to build an independent case, right? Are there, for example, blinding procedures so that individuals who are then doing a subsequent lineup don't know that facial recognition initially matched the individual? If not, right, that is not a particularly meaningful independent check.

The last thing I will say is that I think there's an important sort of intersection here between facial recognition technology, and what we already know about the fallibility of eyewitness identification, right, which, in over 75 percent of known DNA exonerations, there were now known to be wrong eyewitness identification that occurred.

So, that is an investigative tool that itself is already quite fragile, right? When used as a corroborating piece of evidence with the fragile facial identification, that should give reason for concern as well.

So, thinking about what strictures need to be in place to create a meaningful check on the investigative use of facial recognition is an important regulatory move.

Mr. BIGGS. Madam Chair and Ranking Member Jordan, my time has long expired. Thank you.

Ms. JACKSON LEE. Thank you very much.

It is an issue that warrants a lot of involvement, and we thank our Members.

I'm delighted now to recognize Ms. Demings, the gentlelady from Florida, who as a fellow Floridian on the panel, for five minutes.

Ms. Demings.

Ms. DEMINGS. Let me say good morning to all of you. Thank you, Madam Chair, and thank you, Ranking Member, for this very important discussion. Thank you to all the Witnesses for being here. It is good to have a fellow Floridian on the panel as well, so thank you very much.

As a former police executive, I'm always interested in new technologies that can help to keep the public safe, help to keep law enforcement safe, and improve the delivery of police service, and we know that we have work to do in all those areas.

It was a decade ago that we were testing body cameras at the Orlando Police Department, and while we weren't really sure of the road ahead, I do know that the public was very excited about that possibility. Certainly, it is one of the recommendations that is coming to the forefront now, and so, we should always seek technologies that will enable us to do a better job.

Dr. Alexander, you said that technology has long outpaced attempts to govern it, and I think that is such a powerful statement, because not only does it appear that the use of facial recognition outpaced our ability to govern it, but we also see that with other technologies as well.

Dr. Alexander, you talked about some best practices, until we can find ourselves at a point where we can keep up, if that will ever happen, through regulation and other things. Could you just expand a little bit on some of those best practices?

Dr. ALEXANDER. Well, I think that—and thank you very much, Congresswoman Demings.

I think it is very important for us to recognize that technology does move along very quickly. If we think about the development and the implementation of technology over the last 10, 15, 20 years, or even the last five years, it oftentimes outpaces us as human beings. We are not prepared, oftentimes, for the unintended consequences that comes with the technology that we are all utilizing every day in our lives.

So, yes, we have to develop best practices. What is some of those best practices? I think we can really only clearly define them once we make some determination about the real legitimacy of this facial recognition technology. Look, it can be innocently used with our cell phones just to open it up and conduct our personal business. When it comes to the constitutional right of American citizens across this country, regardless of where they are and what neighborhoods they are in, that becomes more problematic. Can we use it as an investigative tool? You know as well as I do, Congresswoman, oftentimes we might embark upon an investigation where we have zero leads, but maybe we have a piece of this facial recognition that suggests, could that be Cedric Alexander?

What we can't do is what happened to Mr. Williams. We can look, well, let's look into the background of Cedric Alexander a little further. Let's explore some other things that we did not even think about, even had a suspect at all, or a person of interest. The problem even lies there, as I've already stated, is that sometimes, we can identify an individual that may be a likely person of interest, a suspect. If our own implicit biases get in the way, it will overwhelm the entire investigation, and it leads us down this dark path of where now we are really doing injury and hurt to people.

Here's the bigger thing I would mention to all of you in Congress, is that as we go through this place in America right now around police reform, one thing we do not need is a piece of technology that is going to continue to drive a separation between police and community. People want good police. We all want great technology. The idea around this technology really is great. It's well-founded. It has to become more accurate. It has to have the type of legitimacy, trust in this technology that is needed for the American people to feel like it's not going to infringe upon the rights and hurt people in any type of way.

I sit on the National Innocence Project Board, and I understand the importance of DNA technology and how it's used to free individuals, quite frankly, who should have never been incarcerated, like Mr. Williams. We have to do a better job in advancing this technology, but understanding that sometimes the technology

moves along faster than we do as human beings, because we still have got a lot of catching up to do around many of the social challenges we have in our great Nation.

So, I hope in some kind of small way that addressed your question, Congresswoman.

Ms. DEMINGS. It did. Thank you so much again. Thank you to all our Witnesses.

With that, I yield back, Madam Chair.

Ms. JACKSON LEE. The gentlelady's time—thank you very much—has expired.

We now recognize Mr. Gohmert for five minutes.

Mr. GOHMERT. Thank you, Madam Chair.

I've got to say, this really warms my heart, to hear Witnesses from both sides having so much good input. It was my observation during the Bush years that the Department of Justice was able to convince Republicans—many of them, a majority of them—“No, we don't need any reform right now,” and really push back and convince Republicans that were in charge to back off some reforms we should have made.

I noticed resistance like that. I'm sure a lot of pressure from the Obama Administration on Democrats that were in charge not to do some reform that was needed.

So, when I hear the testimony and the questions and hear this in such a great, bipartisan way, something that is so serious, it really does warm my heart. Some great comments and great questions.

Dr. Alexander, I note you're careful to make sure that you note that this technology can be helpful, and then it sends me thinking back about our FBI.

Do you think the technology on recording statements, instead of the FBI having their agents not record statements, audio, or video, but just write down their version of what the Witness, do you think the technology has gone too fast for the FBI, that maybe we could get them to start recording with audio at least, maybe video? I am being sarcastic.

That is an area of concern for me. If you combine facial recognition mistakes with the FBI's ability to only record, only write down what their version of what a Witness says, you combine flaws like that, then we are looking at some serious problems at the Federal level.

I am sure your local law enforcement which you oversaw recorded statements, so that wouldn't be such a problem.

Can you see regulations, Dr. Alexander, that would help us be able to confine facial recognition just to the investigative stage?

As a former judge, I know sometimes law enforcement will come in and they will go, “Now, Judge, this is in the affidavit, but, hey, we did also Well, if you didn't swear to it, I don't want to hear it,” That discrimination of real sworn evidence to unsworn evidence isn't always distinguished by some judges.

Do you see some regulations we could utilize to actually get some teeth into that?

Dr. ALEXANDER. Thank you for that question, Congressman Gohmert.

First, let me say, the FBI has the tendency, has the ability, has the training, and also has the fidelity of a Federal law enforcement agency, that is, well-trusted in everything that they have pursued, particularly around technology. They really stood up on technology, if you go back a hundred years with them, in terms of the work that they did back then, and they do today, forensically.

They do have great capability of being able to access that type of technology and use it in a way that is standardized, one in which they have best practices, one in which they really are the leaders around the utilization, because they use this technology to go after foreign actors who want to do harm to this country or to utilize this even in domestic cases.

Mr. GOHMERT. Dr. Alexander, my time is short, but I am very concerned about some of their abuses. When we see the FISA Court that meets in secret, and then there doesn't seem to be any checks.

Like I say, as a former judge, I'm very offended that some judges have not been outraged, like Mr. Williams' treatment and others. I think that is a problem when the judiciary is not upset enough to actually take action and bring law enforcement into line.

Let me ask, Mr. Tolman, do you see a way to get specific regulations that would discern between investigation and actually going to court and getting a warrant and picking up somebody like Mr. Williams?

Mr. TOLMAN. Yeah, I think you could implement things such as not allowing for the facial recognition technology to launch an investigation, that they would have to have the independent basis to launch the investigation. Then, ultimately, if it went to trial, you could utilize facial recognition technology as additional evidence.

You can't have it the other way around, because then you have concerns about whether the evidence that is corroborating the facial recognition technology is simply influenced by the subjectivity of the investigators.

Mr. GOHMERT. Well, thank you.

My time has expired. Thank you very much, Chair Jackson Lee. I really appreciate this hearing.

Ms. JACKSON LEE. Thank you so very much, Mr. Gohmert. We're more and more finding some common ground. Should be some good opportunity for us to move forward.

I am delighted to recognize now, the gentlelady from Georgia for five minutes. Ms. McBath is recognized.

Ms. MCBATH. Thank you so much, Chair. I really, really appreciate you today.

Thank you to each and every one of you that is here today, and just thank you so much for all your timely resource and information, and your expertise.

I would like to go ahead and just start a really quick question.

Dr. Alexander, looking at how we might regulate facial recognition technology, how can we seek to build trust between law enforcement and the communities that they serve, especially communities of color?

Dr. ALEXANDER. Well, fundamentally, that's where a lot of the issue lies, Congresswoman McBath, because currently in the environment that we're in—and this is not new, it's just more exacer-

bated now over the last several years—there is certainly a great deal of mistrust between police and community.

You're already dealing with that in the current context of where we are right now in this country, but as we continue to introduce new technology and ways of seeing things that are questionable, such as facial recognition, if we don't do it right and we end up with continued victims like Mr. Williams, then we continue to create that separation where legitimacy around policing continues to be questioned.

This is the fight that I find myself fighting every day in the roles that I play now, is really trying to build those relationships, but it certainly does have its challenges associated with them.

We've got to get the technology right, because if we don't, it's not going to help the cause in building those relationships. Because if we don't have that collaboration between police and community—and I don't care where it is—we're going to continue to find ourselves here and continue, all of us, to continue to be at risk.

Ms. MCBATH. Thank you so much and stay in the fight.

Dr. ALEXANDER. Yes, ma'am.

Ms. MCBATH. Professor Laurin, your testimony, now it said the rules of discovery, the sharing of case information between the prosecution and the defense are restrictive. So, prosecutors don't actually have to mention what facial recognition technologies they might have used to investigate, and our courts don't get much of an opportunity to advance the law by sorting out what are acceptable and unacceptable uses of this technology.

Could different kind of discovery rules help with this kind of problem?

Ms. LAURIN. Thank you so much for the question, Congresswoman.

I think the short answer is yes. Just at the risk of going a little bit into the weeds, one thing to understand about criminal discovery in the United States, just like criminal law generally in the United States, is that there's tremendous diversity of systems, because we have at least 51 criminal justice systems in the United States, given the States and the Federal government.

So, if you look across those systems, the Federal criminal discovery is really among the most restrictive. Rule 16 is very limited in terms of what information the government is required to disclose to the defense.

There are a number of States that have, particularly in recent years, gone quite in the opposite direction, New York most recently, but my own State of Texas in passing the Michael Morton Act moved to essentially what's called an open file discovery system.

Under that system, the defense typically would have access to essentially the entirety of the nonprivileged, anyway, investigative file, would know the steps that investigators took, regardless of whether the prosecution was going to present that evidence, and regardless of whether a court deemed it to be exculpatory or favorable to the defense.

So, I actually think, in addition to some of the points that Mr. Tolman was just making about regulations that one would want to have in place about how evidence could be used, particularly in thinking about the Federal system, that thinking about opening

discovery more with regard to facial recognition technology is really an essential part of achieving transparency and really vetting the reliability of this in the course of criminal adjudication.

Ms. MCBATH. Thank you.

In just the few moments I have left, Professor Friedman, should Congress regulate private and government-owned systems? I guess I know that the GAO report shows, as others have noted today, that facial recognition systems owned by the government, as well as those owned by private companies and used by government actors, aren't always regulated. Does the ownership of these systems play a role in how they are used?

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

I think it's essential that there be regulation. In fact, I think you're hearing all of us say that it's essential that there be regulation. The likeliest way for Congress to regulate is actually the vendors, the manufacturers of the products that are distributing on the interstate commerce. That's a constitutional hook to get at the regulation. So, I think it's essential.

Now, you do want to regulate the use of those technologies by law enforcement agencies. There's been a lot of discussion about trust between communities and law enforcement, but you're just not going to see that until there's a serious set of regulations for how the technologies are used with very strong guardrails. Again, I could say more, but I see the time has expired.

Ms. MCBATH. Well, thank you so much, each of you.

I yield back the balance of my time, which there is none. Thank you.

Ms. JACKSON LEE. Your time has expired. Thank you so very much.

I now recognize Mr. Tiffany for five minutes.

Mr. TIFFANY. Thank you very much, Madam Chair.

Ms. Frederick, I want to just frame my question with the background that the Biden Administration is reported in the last couple of days to be coming out that they're going to enlist the wireless phone carriers to vet people's text messages.

I mention that because some of my constituents believe we are a short leap to the Chinese Communist Party's use of technology in their country where they have created their social credit system.

Are my constituents right to be concerned about where we're at here in the United States?

Ms. FREDERICK. Well, I will say, as somebody who worked in the intelligence community for almost a decade, I think your constituents are right to be concerned about where these technologies can take us.

What I think is particularly disconcerting is what you mentioned: SMS contents potentially being parsed. Email content has been mentioned as the next frontier. Podcasts have been mentioned as having a portion of unfettered conversations.

These are bastions that shore up our culture of free speech. I definitely think it is of concern to see where authoritarian governments are taking us. Again, we have that system of guardrails.

It is important, especially for conservatives and those expressing heterodox views, to be vigilant and to watch where this technology

naturally goes and guard against it. I think we're all advocating here for certain guards in some respect.

Mr. TIFFANY. Dr. Alexander, you mentioned the State of Maine, in particular Portland, Maine. We also heard from Mr. Lee, commented communities have not been involved.

Isn't there a role for city councils, State governments, those governments that are at the State and local level to get involved with this? Because they're responsible for their police forces in all instances, correct?

Sir, I think you are muted.

Dr. ALEXANDER. Yes, thank you, Congressman.

Yes, you are absolutely right, because there at the local level is where it all starts, in locally elected officials, mayors, city managers, county managers, whatever the case may happen to be. They certainly do need to have a voice in this.

Because what you want to always make sure of is that your police agencies are operating at the highest level of training and certifications. We don't have that yet across the country, and that's why you find some communities that are backing off of this technology until more concrete findings are done.

Mr. TIFFANY. Yeah. Thank you very much for that.

I am just thinking about local elected officials. I have many constituents, though I am in the Wisconsin, that work in the Twin Cities, in Minneapolis. I mean, we saw a real failure on the part of in particular the mayor of Minneapolis and the city council in addressing the riots that overwhelmed the city of Minneapolis last year. A lot of it is because they didn't take control of their police department. There were a few bad cops in that police department, and they needed to take care of them. They did not do it.

This is the same thing. They need to address the technology. It isn't just the city of Minneapolis. It's cities across the country, as well as States. They have the purview, they have the obligation to oversee their police departments, and they should do that, including in regard to using this type of technology.

Final thing that I would say before I am going to yield to Mr. Biggs.

This is the example of the limits of technology. I think about simple things, like with children. They get better reading retention when they read off from paper versus off from an electronic format.

I think about police the same way here. You cannot replace boots on the ground and good investigative work with technology in all instances.

I yield to Mr. Biggs.

Dr. ALEXANDER. That's correct.

Mr. BIGGS. I thank the gentleman for yielding.

My question for you, Mr. Tolman, is this. U.S. Capitol Police has been given Army surveillance equipment to start monitoring Americans. We have a report from a group called Surveillance Technology Oversight Project that says that they think that represents an expansion of police power and surveillance.

Since I just have a few seconds, and then I am going to get to ask the question to you, they point out the expansive nature of the surveillance state.

How do you see this role of actually using military surveillance, giving equipment and technology to law enforcement? How does that expand the surveillance State?

Mr. TOLMAN. Well, in this particular instance it's of grave concern because right now the Capitol Police are exempt from the Freedom of Information Act. So, not only would it be difficult under rules of discovery for a defense counsel, you also would not be able to get transparency.

So, it creates a very powerful surveillance State in an agency that probably is unaccustomed and does not have the history of being these surveillers of United States citizens. So, it's a recipe for disaster.

Mr. BIGGS. Thank you.

My time has expired, Mr. Tiffany.

Mr. TIFFANY. Yes. I will yield back with just one final thing.

I think we should put in the mix here what is happening with these text messages, that they're talking about enlisting the phone companies, the wireless carriers, to intercept people's SMS messages. I think that's a very chilling thing and that should not be done by the Biden Administration. We should throw that into the mix in dealing with this issue as we go forward.

Thank you very much, Madam Chair.

Ms. JACKSON LEE. Well, thank you very much. I know that these issues reach beyond Administrations and deal with important questions that this Committee is now bringing forward. Thank you so very much.

It's now my pleasure to yield to the gentlelady from Pennsylvania, Ms. Dean, for five minutes.

Ms. DEAN. Thank you, Madam Chair. Thank you for convening this hearing on innovative technology and its appropriate use and regulation under the law.

I also thank all our testifiers and advocates today for the enlightening things that you're able to share with us.

Mr. Lee, I would like to start with you. Companies like Clearview claim that through their database it can instantaneously identify people with, quote, "unprecedented accuracy." Yet, Mr. Williams' story isn't unique. Such technology has resulted, as we know, in at least two false arrests in Michigan and one in New Jersey.

Organizations such as ACLU have expressed concern around the risk that Clearview's technology may have on undocumented immigrants, communities of color, survivors of domestic violence, and other vulnerable people and communities. Could you share with us some of the dangers of this face print and its misuse?

Mr. LEE. Absolutely. Thank you for the question, Congresswoman.

There are a number of civil rights and civil liberties concerns with private access to law enforcement investigations, and also with law enforcement's ability to purchase private data. There is little to no transparency, as we said before.

I think a fundamental issue that we need to talk about with respect to this hearing is that these technologies are not accurate, and I think we are having a conversation as if they are. There are

significant error rates across the spectrum, particularly for marginalized and multi-marginalized communities.

So, with little oversight, with little guidance, with no community input, and no meaningful ways to engage in checks and balances, any conversation around the use of facial recognition technology within the criminal legal process is something that The Leadership Conference and many advocacy organizations push back against wholeheartedly.

We should be thinking about a way in which to envision law enforcement and community engagement with law enforcement that does not require surveillance, near-constant surveillance, nor near-constant over policing. That is something that we need to push forward towards.

Ms. DEAN. Thank you so much for that. So, transparency, recognition that this is not a foolproof technology, and the error rate, there's an awful lot more we need to learn.

Mr. Williams, of course we are all moved by your story. Your young daughters watched as you were arrested for a crime you did not commit.

How did your arrest and detainment affect your children, family, and community?

Mr. WILLIAMS. Thank you for the question.

Well, it mainly affected my oldest daughter. My other daughter was only two, so she didn't know what was going on. She cried, too. She just was crying because her sister was crying.

Like I said earlier, I was trying to tell the story. It was a short time. We thought about taking her to see a psychiatrist because every time she sees the story on TV it makes her very emotional and she starts crying, telling us to turn the TV off. I am like, "I am not going to jail every time you see it on TV, baby. It's just they're reporting the story again."

I had wrote something down when somebody else had asked a question. The police actually did investigate it. With all those eye-balls on the pictures, nobody said, "These two guys don't look alike." I don't know how the human part goes into it, but—

Ms. DEAN. Have you ever heard any explanation for that?

Mr. WILLIAMS. No. Nobody told me anything.

Then we basically had to—well, I can't say force them, but we asked them over and over and over again for a proper explanation or a way to say it with some type of—I don't know what the word for it is. They just didn't seem like they were sorry. Like, they didn't want to be apologetic about it. They were like, "It happens. We made a mistake." I'm like, "That doesn't do anything for me, because all I did was come home from work and got arrested."

Then, it's other stuff, like I didn't get dinner that night. They had already served food at the prison. So, I got off work, I got to go sit in a cell with no food and no drinking water. It was terrible for somebody that—I wasn't ready for it.

Ms. DEAN. I have to say, Mr. Williams, thank you for sharing that with us. I asked about your children, but we have to realize what impact this has had on you, a long-term impact on you, to be picked up after work and arrested and detained so inhumanely and so incorrectly.

So, thank you, Madam Chair. I see my time—

Mr. WILLIAMS. I didn't mean to cut you off. I don't know if you can hear that I got a small speech impediment right at this moment. Last year, I also suffered some strokes. They're looking into that to see what actually caused the strokes. I have no idea at this point. I had one doctor say it could have been attributed to stress or whatnot. I don't know if he has a way to prove it. I don't know. I did have strokes last year after.

Ms. DEAN. God bless you.

Mr. WILLIAMS. Thank you.

Ms. DEAN. Please, I pray for your restored health.

Thank you. I yield back.

Ms. JACKSON LEE. Thank you. The gentlelady's time has expired.

Mr. Williams' story should inspire all us, among others, to finding a bipartisan pathway forward.

Let me now yield five minutes to Mr. Massie.

You're recognized, Mr. Massie, for five minutes.

Mr. MASSIE. Thank you, Madam Chair, for holding this very important hearing on a very important topic.

Before I jump into facial recognition, I want to talk about name recognition.

Imagine a system, a computerized system, that instead of basing the adjudication of your civil rights on the distance between your eyes or the shape of your nose or where your ears are in relation to your cheekbones, it's based on the spelling of your first and last name and your birthday and whether you might share a same name with somebody who has been convicted of a felony or may be in prison today.

Well, such a system exists, and there is no judge or jury involved. It's called the NICS Background Check System.

The troubling thing about facial recognition as it exists today, is there may be racial disparities in it. We know that there are racial disparities in the NICS Instant Background Check System. That's the system that you have to go through to purchase a firearm.

My friend John Lott, who worked at the DOJ recently, has found evidence that this system by a factor of three to one produces false denials for Black males compared to White males because they may share a similar name to somebody who is incarcerated within their ethnic group.

So, Ms. Goodwin, I appreciate the good work that the GAO does. You all do great work. I served on the Oversight Committee. We covered this topic before there, the facial recognition topic.

The GAO released a report that said there were 112,000 denials based on the instant background check and only 12 Federal prosecutions. Ostensibly, 100,000 people committed a crime by trying to buy a firearm when they were ineligible.

What we know from that is actually that they didn't commit a crime, but there were a lot of false positives.

I got the commitment of FBI Director Wray in one of our recent hearings to look into this issue about whether there are racial disparities built into the Instant Background Check System. This is not very technologically advanced at all. He said he would work on it.

I hope that this comes across your desk and that you have an opportunity that you might look into it. Is this something that your part of the GAO would examine?

Dr. GOODWIN. Thank you, Congressman. Actually that was my report. I worked on that report.

Mr. MASSIE. Excellent.

Dr. GOODWIN. The prohibited purchases report. So, we are happy to have a conversation with you about additional work we can do in that area.

Mr. MASSIE. Wonderful. Thank you so much. Thank you for that report.

They do collect race information on the Form 4473. So, if we could just take another level, it wouldn't have to be as deep and thorough as the report that you did already, but it would be very helpful, I think.

I noticed that the beginning of this recent report on facial recognition—or your testimony—started with: We surveyed 42 Federal agencies with law enforcement employees or internal law enforcement. I thought, “Whoa, whoa, whoa, stop right there.” That to me is troubling, that we have 42 Federal agencies that have law enforcement.

Maybe this is something the Democrats and Republicans could get together on. Maybe we have too many organizations. If the Department of Education has a police force, then maybe we have too many police forces at the Federal level.

Moving on, I wanted to ask one of our professors here, maybe Professor Laurin, about Brady material, possible exculpatory evidence that's produced and that the prosecution may not want to share with the defense.

You mentioned that the way they get around some of the typical safeguards is they say, “Oh, we just used it to identify the suspect and we're not using it for the conviction.”

Can you talk about how that's problematic and whether defense attorneys can get Brady material from facial recognition companies?

Ms. LAURIN. Thank you for the question.

I'll start with the last piece that you mentioned, which is getting Brady material from companies. In other words, there may be instances, assuming a world that we don't quite live in yet, where facial recognition matches, say, are actually introduced in evidence in a criminal case.

In those instances, the defense would certainly want to, and a competent defense would, sort of interrogate: What's inside the Black box that generated this match?

Well, one of the complicating features here is the proprietary nature of many of these technologies.

So, we haven't seen this yet so much in the facial recognition context, but we have seen it actually in the context of DNA with certain more novel analyses of low copy DNA, et cetera, where the defense has been denied the ability to access the source code, access what is claimed by companies to be proprietary information protected by trade secrets. That intellectual property law has been invoked to quash defense subpoenas.

So, one of the many complicating features here, one of the many limits on the ability of the defense to vet this in a criminal context, is this proprietary dynamic.

Layered on top of that are a number of complications that derive from Brady doctrine and disagreement over the scope of Brady and deciding when defendants are entitled to what we would call Brady material *ex ante* versus after the fact.

I know you have limited time. I am happy to pause there.

Mr. MASSIE. I see my time has expired. I just want to say, I hope Congress will weigh in on this instead of, like the Brady doctrine, allowing the courts to write this for us, because it does seem to be a problem not just within facial recognition, or yet, but with—across all the domains.

I yield back.

Ms. JACKSON LEE. Thank you very much.

I now recognize the gentleman who has dealt with some of these tech issues from a different perspective, the gentleman from Rhode Island, Mr. Cicilline.

You are recognized for five minutes.

Mr. CICILLINE. Thank you, Madam Chair, for calling this very important hearing.

Thank you to the Witnesses for your really compelling testimony.

I want to begin with you, Mr. Williams. I am just wondering whether—first, thank you for being here. Sometimes we talk about these issues in terms of public policy, and it's good to be reminded this actually impacts people's lives in a very profound way, and your story is one example of that.

My question to you is, did it seem like the police had even bothered to conduct an actual investigation, or did they appear to be relying solely on what the computer told them in connection with your arrest?

Mr. WILLIAMS. Okay. Thank you for the question.

So, they did provide information. Like, I didn't find out any of this until after we went to court. They had a lineup of, I guess, six guys, and none of us looked alike. I was like, "Who put this together?" I am going to guess, because I wasn't there, but somebody picked me and said, "This is the guy right here. Do you see him in this lineup?"

I looked nothing like the other guys. I was actually 10 years older than all the other guys in the pictures. They didn't use my current driver's license photo, they used one from six years ago. Well, at this point it's eight years ago.

Mr. CICILLINE. Thank you.

Director Goodwin, are there specific privacy concerns related to potential data breaches of facial recognition systems that are more concerning than breaches of other systems used by the Federal government?

Dr. GOODWIN. Yes, Congressman. Thank you for that question.

So, yes, there are. So, as I mentioned earlier, your face is permanent, it's distinctive. If that information is breached, it's a lot more problematic and more concerning than if your password is breached, because you can change your password, but you can't change, for the most part, you can't change your face.

So, there are major privacy concerns about what it looks like when the technology—when that information is breached.

Mr. CICILLINE. Thank you.

Mr. Lee, facial recognition systems have varying levels of accuracy, but we know they're especially ineffective in identifying people accurately from communities of color and women.

I am just wondering, is there even any training that might help law enforcement to overcome these inaccuracies, or are they so embedded in the system that we should ban facial recognition outright?

Mr. LEE. Thank you for the question, Congressman.

I think that we need to think about, one, contexts of policing that don't involve surveillance and don't involve overly surveilling marginalized communities and over policing them as well.

Also, I would highlight that one of the things that we need to think about is that the technology doesn't—if the technology can't—is not surveilling or if the technology is not working to the same communities that it is trying to help, is this technology worth using in the first place?

So, that's something that we need to think about, particularly within the context of civil rights concerns. Because, again, Mr. Williams was wrongfully arrested, wrongfully detained for a crime that he did not commit based off of a lineup and setup and use of facial recognition technology that was not authorized by the local government, was not known by Mr. Williams himself, was not understood under any circumstances by the people using it, and had varying levels of accuracy across the board that were not given to Mr. Williams at the time or to the law enforcement—

Mr. CICILLINE. I hate to interrupt you. I want to get to one more question.

Professor Laurin, building on what Mr. Massie was asking about, what Mr. Lee just mentioned, we could just simply require prosecutors to inform a defendant that facial recognition technology was used to identify them in any part of the process. That's one reform we could do.

In addition, we could require that the prosecutors disclose any other matches that are sort of exculpatory, statutorily, as Mr. Massie was saying with respect to Brady. There are things we could do to at least make the process more transparent and hopefully give defendants the opportunity to challenge this evidence.

Ms. LAURIN. I agree. There certainly are other items that could be added to that. For example, to the extent the systems report out confidence levels, that is, something that seems necessary to disclose.

I also think this issue of being able to get at that Black box and actually know what's driving the results, which does then involve these questions around intellectual property, is really an important issue to get at.

Mr. CICILLINE. I just want to say, because the Chair recognized this, part of this is facilitated by the monopoly power of these large technology platforms, the fact that they are unregulated, the fact that they are collecting enormous amounts of surveillance. As Ms. Frederick said, the danger of integrating all this presents real challenges.

So, I think it also requires us to regulate how private companies can provide this technology to law enforcement, and larger questions about how we have to rein in Big Tech. I look forward to following up with Ms. Frederick in more detail on her very compelling testimony.

I yield back. Thank you, Madam Chair, for the indulgence.

Ms. JACKSON LEE. The gentleman's time has expired. Thank you very much.

We have other Members who have yet to ask their questions. So, we will certainly move so that you can be included.

Now, I am recognizing Mr. Fitzgerald for five minutes.

Mr. Fitzgerald.

Mr. FITZGERALD. Thank you, Madam Chair. Thank you very much. Fascinating stuff this morning.

I just wanted to move maybe in a direction of a little bit away from the law enforcement aspect to just the private sector, which some of the Members touched on this morning.

As we see, iPhones that use face recognition. Any time you are going through the airport now, you see the Clear system, which is allowing access for individuals in airports on a regular basis. Then some employers, now that we're reading, are using this in relationship to their employees and under the auspices of security. So, there's a lot of different things happening in the private sector.

The question I had for Ms. Frederick and Mr. Tolman, can you address some of the constitutional and privacy concerns of private sector use, particularly related to the difference between using facial recognition technology for verification purposes rather than just flat-out identification?

Ms. FREDERICK. So, I will start here. I think generally, from a wave-top level, it's that outsourcing of surveillance that portends more concrete, potential concrete violations of the Fourth Amendment.

I'm not a lawyer. I don't profess to be. When I see the surveillance State basically outsourcing this job to private companies that don't fall under the remit of the United States Constitution, that's what starts to worry me as a citizen, somebody who has been behind the powerful technologies that are employed at a commercial level also by the surveillance States overseas.

To me, it's that outsourcing to private companies that we need to think about when it comes to the Constitution, because some reports indicate that is expressly made to skirt the constitutional protections.

So, I'll let Mr. Tolman give his broader expertise on this.

Mr. TOLMAN. Yeah, I think that last point is where I wanted to go, which is oftentimes the use of third-party providers is an end run around the protections. We have already seen one court has indicated that the Baltimore Police Department violated the Fourth Amendment in its use of facial recognition technology. That would be one pressure point to push you towards utilization of a third-party provider, one in which you have a somewhat lower standard when utilizing the evidence from them.

We don't know the nature of some of those partnerships. That's the biggest problem right here, is the lack of transparency in the

information. We don't know what it is, sometimes even the questions we need to ask to find out how pervasive that relationship is.

Mr. FITZGERALD. Thank you. Great answers.

The other question that I would have for both of you would be there's been some discussion about a full-out ban. What we're seeing across the Nation is some municipalities through ordinance have been progressively addressing this issue as it emerges, as part of something that's under their control, many times it is a municipal court system. They're moving forward, city councils and even some county boards are moving forward to full-out bans.

Is that practical at this point? You can probably hear it in my voice. It doesn't seem like it is to me at this point.

Mr. TOLMAN. I would just quickly say that it is hard to imagine that this powerful tool is not to be utilized at all. I understand the calls for bans, but that's what makes this so difficult, is there are circumstances in which this powerful technology may be the only thing that may save a victim or save a town from some horrific crime or from a terrorist attack, for example. So, getting this right in how we do authorize law enforcement to use it is right now the most important job I think this Congress has.

Ms. FREDERICK. I prefer to think of it more—

Mr. FITZPATRICK. Ms. Frederick, do you care to comment on that.

Ms. FREDERICK. Yes, sir. I prefer to think of it more as a tactical pause, take the time to get it right. So, I think there are measures with which we could do so.

Lawsuits are being fought in the courts as well. ACLU is suing Clearview AI. Its Illinois arm filed a 2018 lawsuit against Chicago Police. So, there's other mechanisms as well as municipalities to take that tactical pause, take the time to get it right.

Mr. FITZGERALD. Thank you.

Thank you, Madam Chair. I yield back. Thank you.

Ms. JACKSON LEE. I thank the gentleman.

I am now pleased to recognize the gentleman from California, a former AUSA, Mr. Lieu.

You are recognized for five minutes.

Mr. LIEU. Thank you, Chair Sheila Jackson Lee.

I am super excited that you called this hearing. My office and I have been working on facial recognition for over two years. The reason it's taken so long is, as the Chair has aptly stated, it is a can of worms. When you look at this issue, it can get very complicated.

We have worked on legislation that is essentially complete now. It basically requires a warrant for most cases of the use of facial recognition technology. It sets auditing and bias testing standards. It requires reporting. It prohibits facial recognition technology for most First Amendment-protected activity. There are a number of other provisions.

We're going to circulate that legislation to the Members of this Committee, both Democrats and Republicans, for your review and comment and coauthorship.

So, thank you, Chair Lee, for this hearing.

My first question goes to Professor Laurin.

We already know from this hearing, facial recognition technology implicates the First, Fourth, and Fifth Amendments. I want to talk

about the Equal Protection Clause, because there is this disparity in accuracy in terms of the color of your skin. Would there also be an equal protection violation if we had government agencies deploy this knowing that similarly situated people are being treated differently in terms of surveillance?

Ms. LAURIN. So, thank you very much for the question.

I think that in answering the question I want to sort of distinguish between constitutional doctrine as it stands and maybe a more intuitive sense of what is rightfully understood to be constitutionally problematic.

So, I think the challenge with using the Equal Protection Clause and the doctrine around it to get at these issues of bias in facial recognition is that existing Supreme Court doctrine requires that essentially discriminatory intent be proved for State action to be deemed to be a violation of the Equal Protection Clause.

That presents a hurdle when one is working with evidence of disparate impact. There's an evidentiary gap often in getting from the State realizes there's a disparity to the State wants to discriminate on the basis of race or on the basis of sex. That has been a real difficulty in using the courts to get at these problems of disparity.

Now, that doesn't mean that it wouldn't be understandable, appropriate for Congress to say, "We see a problem in these disparities," and want to legislate to require that disparities themselves be sufficient basis for limiting the use of technology, et cetera. Of course, one needs to think about what the hook would be for that in terms of section 5 or the Commerce Clause or something along those lines.

I think that existing doctrine presents a challenge because of this requirement of discriminatory intent.

Mr. LIEU. Thank you. I appreciate that.

My next question goes to Professor Friedman.

First, let me take a step back and say I do agree with Dr. Alexander and Mr. Tolman that we can't just ban this technology. If you look at the course of human history, nearly impossible to ban technology. We can regulate it.

Professor Friedman, because there's so many different iterations and possible uses and situations for facial recognition technology, what do you think about imposing a warrant requirement that can actually take into account all the different particularized factors before deciding whether any specific case we would use facial recognition technology?

Mr. FRIEDMAN. Thank you for the question.

I just want to make a comment about the ban versus moratorium or strategic pause point, which I think everybody is recognizing. We got the cart ahead of the horse here, and that's the problem. So, regulation is the only shot we have of getting the horse back out in front.

Warrant requirements are useful in some circumstances and not others, and it depends on the use case for the technology. So, for example, if the use case is identification, which is what most agencies are doing right now, they take a probe photo and they compare it to a database, a warrant requirement makes sense, but only to get permission to use the technology because there is a reasonable belief that the photo that you have got is somebody that is sus-

pected of a crime that is permitted under the statute. I, for one, would only allow the use facial recognition for very serious crimes.

So, that is a use of the warrant that makes sense. The warrant can't tell you, for example, that a particular individual committed the crime. It's just to use the technology.

Mr. LIEU. Great. Thank you.

I see my time is up, and I yield back.

Ms. JACKSON LEE. The gentleman's time has expired.

I think we have present with us the distinguished gentleman from Utah.

Mr. Burgess Owens is recognized for two minutes.

Mr. OWENS. Thank you, Chair Jackson Lee and Ranking Member Biggs. Thank you for holding this very important hearing today.

The concerns surrounding facial recognition technology demand a bipartisan solution, and I look forward to working with my colleagues to address these concerns.

I'd like to thank the Witnesses today.

Mr. Williams, we all agree on the unfairness of what you and your family have had to endure. Thank you so much for your decision to stay in the fight, to share your experiences, and do your best to make sure no other Americans have to experience what you and your family are going through.

I'd also like to give a special welcome to my friend and fellow Utahn, Mr. Brett Tolman. Along with other accomplishments mentioned previously, Brett has also been a very strong advocate of criminal justice reform.

I am finding the upside of being toward the end of the questioning is the remarkable education that a person received over the last couple of hours. The downside is the questions I had coming into the session have been answered. So, I am going to yield the remainder of my time back to Ranking Member Biggs.

Before I do, I would like to highlight something that was mentioned previously, and that is the heartwarming bipartisan concern that I am feeling and seeing as we go through this topic.

I'd also like to point out that as we do confront solutions of solving the increased crime that we are seeing everywhere that we cannot rely on technology. Technology is our tool to help support human relationships, and all human relationships are based on respect.

We cannot continue to demean and disrespect the good servants, the 90 percent of good men and women policing our communities and expect technology to make up for it.

I am convinced that this Committee will find the solutions and address the concerns of facial recognition technology. Let's take the same passion to bring back the respect for our law enforcement officers, men and women, the same respect that I had when I experienced it as a child. Our communities will have the benefit of more confidence in our future innovations once we have that accomplished.

With that, I would like to yield back my remaining time to Mr. Biggs.

Mr. BIGGS. I thank the gentleman for yielding, and Madam Chair.

Just a couple of quick points. This has been a very enlightening hearing. We have not really addressed, in my opinion, enough the question on reasonable expectation of privacy that's been shattered by the data scraping that goes on by private concerns to develop these databases which are being referred to.

I hope that we can expand our investigation into that, because I don't think the question has been settled through the courts yet either. If it has, I haven't seen it. We certainly need to get to that.

I also want to comment on Mr. Lieu's legislation.

I look forward to reading it, Mr. Lieu, and I appreciate your efforts on it. I hope that we can also integrate some of the work that was done in the previous iteration of the OGR Committee with Chair Cummings and working on that as well. So, I look forward to seeing it, Mr. Lieu, and hope that you can get that to us soon. I appreciate it.

When I want to ask Mr. Tolman this question because it really gets to the heart of some of what we're talking about. This is just, as Mr. Lieu said, this is a can of worms when you open this thing up.

When we start bringing together other technologies, we have discussed this SMS and email, and we have moved from just using this mere identification, which is in and of itself a problem, to the potential to track movement, this notion of science fiction-type, pre-crime, and stopping pre-crime.

What's your take on that, in a very brief way, that we're on a spectrum that's going to keep moving to trying to stop people from committing crimes before a crime is ever committed using this technology and others combined?

Mr. TOLMAN. Yeah, I share the concern. We have seen that when law enforcement is given additional technology their first instinct is to utilize it because they have a sincere and genuine desire to work on behalf of our communities and the victims of crime.

However, they are often the last one to actually ask the question: Should we utilize this technology? That has to be the reasoned discussion of Members of the legislature that identifies this.

We are already seeing that speech and social distancing under COVID and areas where we have not ever been, are now areas where we are focusing law enforcement technology and action. Because of that, we're on a slippery slope, and I would share your concern.

Mr. BIGGS. Thanks, Mr. Tolman. I hate to cut you off, but I want to finish from our side where we started with the Chair, and that's the testimony of Mr. Williams.

So, Mr. Williams, in your testimony, your written testimony, you said, quote, "I don't want anyone to walk away thinking that if only the technology was made more accurate its problems would be solved," close quote.

Well, I think the issues which we have discussed today are not just issues with accuracy of the technology. I think we're talking about a total invasion of privacy, which is absolutely unacceptable, which at some point is going to give too much power to the state. We had actually seen it already in your case, Mr. Williams, and others that we have discussed today.

So, I am looking forward to working with the Chair, Mr. Lieu, and others on this Committee who have a sincere interest in resolving this issue.

Thank you, and I yield back.

Ms. JACKSON LEE. Thank you, Mr. Biggs. You are absolutely right, we have a sincere interest in resolving this issue, and there are layers of issues that we can respond to as a Committee in a bipartisan manner.

Speaking of bipartisanship, I'm delighted to yield to the gentleman from California, a former sheriff, Mr. Correa, for five minutes.

Mr. CORREA. Thank you, Madam Chair, for holding this most important hearing.

I want to thank all our Witnesses today for some very good testimony.

Mr. Williams, I will also say, hearing your story, being in a cell for 30 hours, not knowing why or what you were accused of, is alarming, tragic at many levels.

As we think about society today, when you give your fingerprints, you give permission to have your fingerprints taken. When you go in for a live scan, you say, "Here are my prints, take the scan." When you give your DNA, you give it with permission, knowing that somebody is going to do a DNA scan on you.

When it comes to facial recognition, no consent is necessary. In fact, most people don't even know that their information, their facial information, is being collected by somebody, a private entity out there.

Mr. Bertram Lee mentioned that 133 million Americans—let me repeat that—133 million Americans have their facial recognition data in a database some way or another in this country. I presume that most, if not all, gave that information or gave their facial information without any consent or even them knowing that data was taken from them.

So, Professor Laurin and Professor Friedman, today I have a question for you. We discussed the Constitution, our rights. In effect, are there any regulations, laws that govern to limit in any way possible a private entity's ability to collect facial recognition data? As a taxpayer, as a citizen, am I going to have to accept the fact that a private firm has my facial recognition data to sell or use as they wish? Question.

Mr. FRIEDMAN. Professor Laurin, if I may?

Ms. LAURIN. Please go ahead.

Mr. FRIEDMAN. I just want to appreciate the question at a couple of levels because I think it's so critically important.

It's very easy to fall into the language of constitutional rights here, and the constitutional rights are, obviously, critically important. The interpretation of the Constitution by the courts often doesn't touch the things that we're talking about, in part because the technology is rushing ahead of the courts.

So, you could not be more correct that there is an urgent need for regulation, for legislation, both as to private companies and as to law enforcement agencies.

Then as to the private companies, I don't know of any congressional law that deals with this. Some States have stepped in, like

Illinois in this space. For the most part there's a void. I think the need for legislation is essential.

Mr. CORREA. Ms. Laurin?

Ms. LAURIN. I can really only essentially echo what Professor Friedman said. He speaks my mind. I think that there is a tendency, actually, to overly prioritize the constitutional stuff and to miss the fact that actually the Constitution is a floor, not a ceiling, in terms of protections.

In fact, often the constitutional protection is lower by design because the courts say really there are details for Congress to figure out, it's really not our institutional place.

Mr. CORREA. So, I will ask you again. Let me repeat my question.

As a taxpayer, as a citizen, am I going to have to accept the fact that right now a private third party has my facial recognition information and they can do whatever they want to do, sell that information to whoever they want to sell it, without any repercussions, without any regulation, without violating any kind of a law? Is that the case? Is that the State of the laws in this country today?

Ms. LAURIN. The best answer I can give you, without presenting myself as an expert in every statutory scheme governing, for example, electronic communications, et cetera, is that I do think that there are at least some data privacy regimes, statutory data privacy regimes that would limit some activities.

In the main, there is very little regulation currently. Certainly, the Constitution has virtually nothing to say about private nonstate action. That is why congressional action is so important.

Mr. CORREA. So, I'm left here with a very unsettling feeling that I essentially have no remedy for somebody using my facial data recognition information for whatever they want to do with it?

Mr. FRIEDMAN. Well, you can create one. You have the—Congress has the power to regulate products moving in interstate commerce. You could change that state-of-affairs if you chose to.

Mr. CORREA. Thank you, Madam Chair. Ran out of time. I yield.

Ms. JACKSON LEE. The individual ran out of time. Mr. Correa, we are all running out of time. This is such an important issue, and I'm very grateful for all my Members. I listened to—as I yield just for a moment, I listened to Professor Friedman over and over again about regulation, and that is what we are having this hearing for, because we are working on legislation, and I look forward to working with Mr. Biggs, but also with our colleagues who are, likewise, working on legislation to be able to address the question of a regulation or a construct that needs to address this question. So, thank you all very much.

It's my pleasure to yield to the Vice Chair of this Subcommittee from Missouri, the gentlelady, Congresswoman Bush, for five minutes.

Ms. BUSH. Thank you, Chair, for convening this hearing.

We as a Committee have spent significant time addressing the brazen and broad scope of power held by law enforcement agencies, from the FBI to various prosecutorial entities under the Department of Justice. Time and time again, we are met with concrete examples of unfettered law enforcement practices that not only undermine our fundamental civil liberties, but our basic principles of human dignity and security.

When the ACLU conducted a study with Members of Congress and a mug shot database, 28 Members of Congress were falsely matched, including the late Congressman John Lewis, and this was Members of Congress, public officials. Imagine what it's like for everyday people across this country.

What we do know of this technology is that the darker your skin tone, like mine, the more likely you will be falsely identified.

During the Ferguson uprising following the murder of Michael Brown, Jr., I recall wearing bandanas as a response to the tear gas. It was during that time, though, that we realized that we needed to wear bandanas because of the likelihood of facial recognition technology being used against protest movements and surveilling each and every one of us involved in the Ferguson uprising.

Director Goodwin, the GAO found that 14 agencies reportedly use facial recognition technology to support criminal investigations. Yes or no, was FRT used by the Federal law enforcement agencies during the protest following the torture and murder of George Floyd? It's just a yes or no.

Dr. GOODWIN. Yes.

Ms. BUSH. What are the collateral consequences of protestors being identified by these technologies?

Dr. GOODWIN. So, Congresswoman, we didn't go into that issue, but we raised the concerns about privacy and accuracy. So, of course, with accuracy, the concern is that people would be misidentified by the technology, and that could have adverse consequences. The privacy issue is that there are faces. A person's face could be out there and could be used a number of ways. So, our focus was to look at the lay of the land for how law enforcement were using the technology.

Ms. BUSH. Thank you.

In 2016, it was reported that police used facial recognition to surveil crowds during the Freddie Gray protest to find people with outstanding warrants.

Mr. Lee, are there any protections for protestors' identities when they are in public spaces but engaging in First Amendment-protected activity?

Mr. LEE. Thank you for the question, Congresswoman.

This would be, in our mind, a clear violation of the First Amendment. Also, there are serious privacy and civil liberties concerns with the use of facial recognition technology that we saw not only with the George Floyd protest, but also that we saw in LAPD using Ring cameras to surveil Black Lives Matter protestors. We have serious concerns, and there are serious civil rights and liberties concerns about the tracking of protestors, especially in these circumstances and especially when the technology is not well-used or very accurate.

Ms. BUSH. So, Mr. Lee, how does the use of the facial recognition technology used to identify protestors? How does that influence the public's perception or opinion of law enforcement, or even the high-tech policing?

Mr. LEE. There's already a tenuous relationship between communities that are over-surveilled and over-policed in law enforcement. We have seen this time and time again over the past year, and that is something that I think Congress needs to keep in mind when

looking about regulating facial recognition technology. These are tools used by law enforcement to disproportionately target Black and Brown people across the Nation, and we need to keep that in mind, and the civil rights and civil liberties of those people in mind, as we think about what the next steps are. That is why we, as a civil rights community, have asked for a ban or a moratorium and a tactical pause, to use the language of Ms. Frederick. We think that it chills protests. It chills speech. It misidentifies, and it does not work.

Ms. BUSH. Thank you so much, Mr. Lee.

There are local solutions that are being [inaudible].

Ms. JACKSON LEE. Ms. Bush—are we able to get Ms. Bush connected?

I think we may have lost Congresswoman Bush.

Thank you very much, Congresswoman, for those insightful, very insightful points that you have raised. I have been impressed by the direction of our questions, the depth of our questions, and, certainly, the importance of our Witnesses.

Mr. Biggs, I have questions that I'm going to utilize at this time, but I'm happy to yield to you have been certainly rewarded with time. I'm happy to yield with you before I make my final inquiries that I hope will be important to the record of this hearing and proceedings.

Mr. Biggs?

Mr. BIGGS. Thank you, Madam Chair. I know you will be surprised to hear this, but even though I have many more questions and comments about this, I appreciate those that have participated; but I'm going to limit my comments right there and, again, thank the Members, the Witnesses, and yourself.

Thank you, Madam Chair. I yield back.

Ms. JACKSON LEE. Thank you so very much and thank you to the Witnesses.

I'm going to proceed with some questions that I did not proceed with. As I do so, I want to make sure that I thank all the Witnesses again. You will probably hear me thank the Witnesses more than once.

I would like to submit into the record—and then I will begin just some questions that I think are very important. I want to submit into the record the GAO report that I believe was entitled, “Facial Recognition Technology, Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used by Employees.” I think that is shocking, and I think that is also indicative of what I think Dr. Alexander made mention of in terms of the numbers of law enforcement and the utilization of this tool without training.

[The information follows:]

MS. JACKSON LEE FOR THE RECORD



United States Government Accountability Office

Testimony
Before the Subcommittee on Crime,
Terrorism, and Homeland Security,
Committee on the Judiciary, House of
Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Tuesday, July 13, 2021

FACIAL RECOGNITION TECHNOLOGY

Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees

Statement of Greta L. Goodwin, Director,
Homeland Security and Justice



FACIAL RECOGNITION TECHNOLOGY

Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees

What GAO Found

In June 2021, GAO reported the results of its survey of 42 federal agencies that employ law enforcement officers about their use of facial recognition technology. Twenty reported owning systems with the technology or using systems owned by other entities, such as state, local, and non-government entities (see figure).

Ownership and Use of Facial Recognition Technology Reported by Federal Agencies that Employ Law Enforcement Officers

Owned system	Used another entity's system		Owned system and used another entity's system		
 Department of Veterans Affairs Police Service	 Bureau of Alcohol, Tobacco, Firearms, and Explosives	 Bureau of Diplomatic Security	 Drug Enforcement Administration	 U.S. Customs and Border Protection	 Federal Bureau of Investigation
 Federal Bureau of Prisons	 Food and Drug Administration, Office of Criminal Investigations	 U.S. Fish and Wildlife Service	 U.S. Immigration and Customs Enforcement	 Pentagon Force Protection Agency	 U.S. Secret Service
 National Aeronautics and Space Administration, Office of Protective Services	 Internal Revenue Service, Criminal Investigation Division	 U.S. Capitol Police	 U.S. Marshals Service	 Transportation Security Administration	
	 U.S. Park Police	 U.S. Postal Inspection Service	 U.S. Probation and Pretrial Services		

Source: GAO analysis of survey data. | GAO-21-105309

Note: For more details, see figure 1 in [GAO-21-105309](#).

Agencies reported using the technology to support several activities (e.g., criminal investigations) and in response to COVID-19 (e.g., verify an individual's identity remotely). Six agencies reported using the technology on images of the unrest, riots, or protests following the killing of Mr. George Floyd in May 2020. Three agencies reported using it on images of the U.S. Capitol attack on January 6, 2021. Agencies said the searches used images of suspected criminal activity.

Fourteen of the 42 agencies reported using the technology to support criminal investigations. However, only one had a mechanism to track what non-federal systems were used by employees. By having a mechanism to track use of these systems and assessing the related risks (e.g., privacy and accuracy-related risks), agencies can better mitigate risks to themselves and the public.

United States Government Accountability Office

Chair Jackson Lee, Ranking Member Biggs, and Members of the Subcommittee:

I am pleased to be here to discuss federal law enforcement's use of facial recognition technology. Use of this technology has expanded in recent years, raising concerns about privacy and the accuracy of facial recognition systems. Members of Congress and academics have highlighted the importance of understanding what technologies are owned and how they are used by federal law enforcement.

My statement today will focus on (1) the ownership and use of facial recognition technology by federal agencies that employ law enforcement officers, (2) the types of activities these agencies use the technology to support, and (3) the extent that these agencies track employee use of facial recognition technology owned by non-federal entities, including the potential privacy and accuracy implications. This statement is based on findings from our June 2021 report, which included the results of our survey questionnaire to 42 federal agencies that employ law enforcement officers about their use of the technology.¹ The report provides a detailed description of our scope and methodology.

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.

Background

Federal and Non-Federal Systems with Facial Recognition Technology

Federal law enforcement may use systems with facial recognition technology owned by their respective agencies. They may also use systems owned by other government entities, including federal, state, local, tribal, and territorial government entities. Moreover, federal law

¹GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, [GAO-21-518](#) (Washington D.C.: June 3, 2021). Our June 2021 report was a public version of a sensitive report that we issued in April 2021 (GAO-21-243SU). Some federal agencies deemed information in our April 2021 report to be sensitive, which must be protected from public disclosure. Therefore, the June 2021 report and this statement omit sensitive information about federal agency ownership and use of facial recognition technology.

	enforcement may use non-government facial recognition service providers, such as Vigilant Solutions and Clearview AI. For example, law enforcement officers with a Clearview AI account may use a computer or smartphone to upload a photo of an unknown individual to Clearview AI's facial recognition system. The system can return search results that show potential photos of the unknown individual, as well as links to the site where the photos were obtained (e.g., Facebook). In some cases, law enforcement officers can access another entity's system and conduct a facial recognition search. Alternatively, law enforcement officers can request that another entity use its system to conduct facial recognition searches on their behalf. For example, federal law enforcement officers may ask a state police department to conduct facial recognition searches on their behalf.
Privacy Laws and Rules	Several statutory requirements govern the protection of personal information by federal agencies, including federal law enforcement's use of facial images. The Privacy Act of 1974 places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records (e.g. photos). According to Office of Management and Budget (OMB) officials, the Privacy Act and OMB Circular A-130 generally provide that agencies must ensure that privacy requirements apply to systems operated by contractors or other entities on behalf of the Federal Government, which could include facial recognition service providers.
Accuracy of Facial Recognition Technology	The accuracy of facial recognition technology can be characterized in a number of ways. For example, a false positive rate is how often the technology incorrectly declares two images to be a match when they are actually from two different people. In addition, a false negative rate is how often the technology fails to declare two images to be a match when they are actually from the same person. Matching errors can be caused not only by the quality of the facial recognition technology, but also by the quality of the photos used in the matching process and other factors. The National Institute of Standards and Technology has conducted research into the accuracy of facial recognition algorithms. It has evaluated hundreds of commercial facial matching algorithms for accuracy and speed since 2000.

Twenty Federal Agencies Reported Owning or Using Systems with Facial Recognition Technology

We surveyed 42 federal agencies that employ law enforcement officers, 20 of which reported that they owned a system with facial recognition technology or used another entity's system.² As shown in figure 1, three agencies only owned a system, 12 agencies only used another entity's system, and five agencies both owned a system and used another entity's system. According to these agencies, some systems can include hundreds of millions or billions of photos.

²Specifically, we asked agencies whether at any point from January 2015 through March 2020, they owned a system with facial recognition technology, including systems in the process of being developed. In addition, we asked agencies whether at any point from April 2018 through March 2020, they used facial recognition technology—that is, their offices, employees, or contractors (1) accessed a system owned/operated by another entity, or (2) requested that another entity use its system to conduct a facial recognition search on their behalf. See the complete list of 42 federal agencies that received our questionnaire in appendix I.

We defined facial recognition technology as a type of automated or semi-automated biometric technology that uses images for verification, identification, and/or investigative purposes. In addition, we stated that a system with facial recognition technology may include a facial recognition algorithm, hardware, software, and a photo database. We asked agencies to include all uses of facial recognition technology in their response except for facial recognition technology that was solely used to authenticate the identity of the agency's employees and contractors to log into computers and phones.

Figure 1: Ownership and Use of Facial Recognition Technology Reported by Federal Agencies that Employ Law Enforcement Officers

Owned system	Used another entity's system			Owned system and used another entity's system	
					
Department of Veterans Affairs Police Service	Bureau of Alcohol, Tobacco, Firearms, and Explosives	Bureau of Diplomatic Security	Drug Enforcement Administration	U.S. Customs and Border Protection	Federal Bureau of Investigation
					
Federal Bureau of Prisons	Food and Drug Administration, Office of Criminal Investigations	U.S. Fish and Wildlife Service	U.S. Immigration and Customs Enforcement	Pentagon Force Protection Agency	U.S. Secret Service
					
National Aeronautics and Space Administration, Office of Protective Services	Internal Revenue Service, Criminal Investigation Division	U.S. Capitol Police	U.S. Marshals Service	Transportation Security Administration	
					
	U.S. Park Police	U.S. Postal Inspection Service	U.S. Probation and Pretrial Services		

Source: GAO analysis of survey data. | GAO-21-105309

Note: We sent a survey questionnaire to 42 federal agencies that employ law enforcement officers. We asked agencies whether at any point during January 2015 through March 2020, they owned a system with facial recognition technology, including systems in the process of being developed. In addition, we asked agencies whether at any point from April 2018 through March 2020, they used facial recognition technology—that is, their offices, employees, or contractors (1) accessed a system owned or operated by another entity, or (2) requested that another entity use its system to conduct a facial recognition search on their behalf.

The owned system columns include systems in the process of being developed. The National Aeronautics and Space Administration's Office of Protective Services reported that it did not purchase facial recognition technology. However, we included the agency in the owned column because it used a commercial-off-the-shelf product with facial recognition technology to conduct a proof of concept test to determine whether the technology was suitable for its purposes.

Eight Agencies Reported Owning Systems with Facial Recognition Technology

Eight of the 42 federal agencies reported owning 17 systems with facial recognition technology, from January 2015 through March 2020.³ Of these systems, four were in operation as of March 31, 2020, and were owned by three agencies: the Federal Bureau of Investigation, Federal Bureau of Prisons, and U.S. Customs and Border Protection. In addition, one of the eight agencies reported that it was in the process of procuring two systems during this time period, but had not finalized the purchase as of March 2020. Detailed descriptions of the 19 systems (17 owned and two in procurement) and their status as of March 31, 2020 can be found in our June 2021 report.

Seventeen Federal Agencies Reported Using Systems Owned by Other Entities

Seventeen of the 42 federal agencies reported using another entity's system with facial recognition technology from April 2018 through March 2020. Of the 17 agencies, 15 reported using systems owned by another federal entity; 14 reported using systems owned by state, local, tribal, or territorial entities; and 11 reported using systems owned by non-government entities. Furthermore, nine of the 17 agencies reported using systems owned by all three types of entities. See table 1 for additional information.

Table 1: Reported Use of Other Entities' Facial Recognition Technology by Federal Agencies that Employ Law Enforcement Officers

Federal Agency That Used System	Type of Entity That Owned System				
	Other Federal	State, Local, Tribal, Territorial	Non-Government ^a		
			Clearview AI	Vigilant Solutions	Other Non-Government ^b
Bureau of Diplomatic Security	✓	✓	✓	✓	✓
U.S. Customs and Border Protection	✓	✓	✓	✓	✓
U.S. Marshals Service	✓	✓	✓	✓	✓
Bureau of Alcohol, Tobacco, Firearms and Explosives	✓	✓	✓	✓	—
U.S. Immigration and Customs Enforcement	✓	✓	✓	—	✓

³This statement omits some information about systems owned by agencies we surveyed, as the relevant agencies deemed the information sensitive.

Federal Agency That Used System	Type of Entity That Owned System				
	Other Federal	State, Local, Tribal, Territorial	Non-Government ^a		
			Clearview AI	Vigilant Solutions	Other Non-Government ^b
U.S. Postal Inspection Service	✓	✓	✓	✓	—
Drug Enforcement Administration	✓	✓	✓	—	—
Federal Bureau of Investigation	✓	✓	✓	—	—
U.S. Secret Service	✓	✓	✓	—	—
U.S. Capitol Police	✓	✓	—	—	—
U.S. Fish and Wildlife Service	✓	✓	—	—	—
Food and Drug Administration, Office of Criminal Investigations	✓	✓	—	—	—
Internal Revenue Service, Criminal Investigation Division	✓	✓	—	—	—
U.S. Park Police	—	✓	✓	—	—
Administrative Office of the U.S. Courts, U.S. Probation and Pretrial Services	—	—	—	—	✓
Pentagon Force Protection Agency	✓	—	—	—	—
Transportation Security Administration	✓	—	—	—	—
Total	15	14	10	5	5

Legend:

✓ Agency used a system owned by the respective entity (or entity type) at any point from April 2018 through March 2020. For federal, state, local, tribal, and territorial entities, the term "used" includes an agency's offices, employees, or contractors (1) accessing a system owned/operated by the respective entity type, or (2) requesting that the respective entity type use its system to conduct a facial recognition search on the agency's behalf. For non-government entities, the term "used" means the agency's offices, employees, or contractors submitted photos to the respective non-government service provider for the purpose of conducting a facial recognition search.

— Agency did not use a system owned by the respective entity (or entity type) at any point from April 2018 through March 2020.

Source: GAO analysis of survey data. | GAO-21-105309

^aSome agencies reported that they only used Clearview AI or Vigilant Solutions on a free trial basis, and thus, did not enter into a formal contract with the service provider.

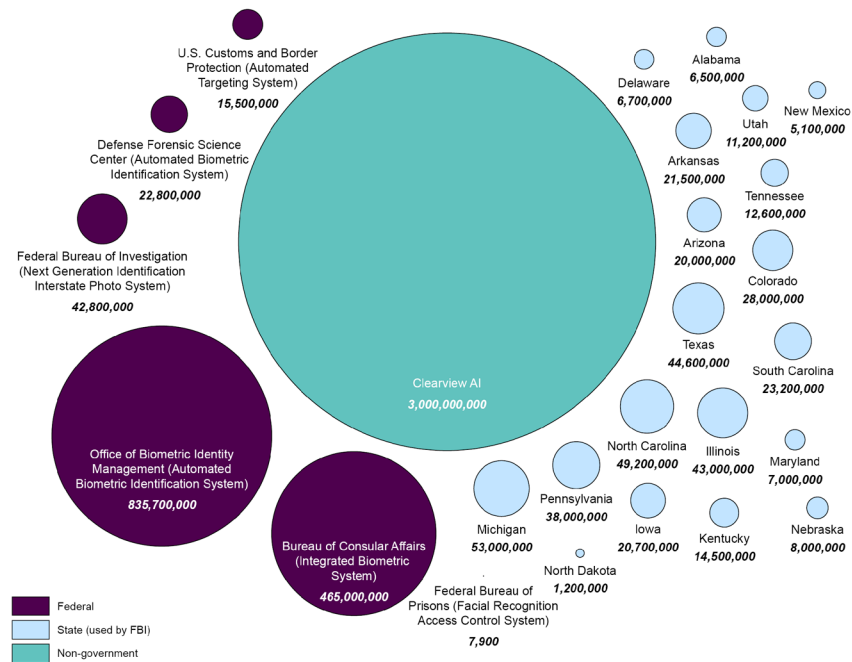
^bOther non-government entities that agencies reported using included Amazon Rekognition, BI SmartLink, and Giant Oak Social Technology, among others.

Agencies Reported Using Systems that Varied in the Number and Type of Photos

Federal agencies reported using numerous systems with facial recognition technology, and sometimes these systems included stored photos. The number and types of photos within these systems can vary, based on information reported by agencies and system owners. Reported photo types included: mug shot photos, driver's license photos, passport photos, publicly available photos on the internet, and images from video/Closed Circuit Television. Figure 2 below shows examples of federal, state, and non-government systems with facial recognition

technology that federal agencies reported using, and the number of photos in them.

Figure 2: Selected Federal, State, and Non-government Systems with Facial Recognition Technology Used by Federal Agencies that Employ Law Enforcement Officers, and the Number of Photos in Them



Note: We sent a survey questionnaire to 42 federal agencies that employ law enforcement officers. This figure includes examples of systems used by one or more federal agencies we surveyed. It does not include all systems used by these agencies. The figure includes the number of photos stored in the respective entity's system with facial recognition technology, as of March 31, 2020.

The same individual may be included in multiple photos within one photo database or across multiple databases, and the same photo can exist within multiple databases. Some entities providing these numbers indicated they were estimates. The number of photos for federal and non-government entities were reported by the respective system owner. The number of photos for state entities were all reported by the Federal Bureau of Investigation (FBI). Specifically, the FBI's Facial Analysis, Comparison, and Evaluation Services has memorandums of understanding with several state agencies, allowing it to leverage the state-owned systems for facial recognition searches. The FBI provided the number of photos they can access via these memorandums of understanding.

Federal Agencies Reported Using Systems with Facial Recognition Technology to Support Various Activities

Federal agencies reported using facial recognition technology to support various activities, such as criminal investigations and surveillance, and also in response to the Coronavirus Disease 2019 (e.g., verify an individual's identity remotely). Of the 20 agencies that owned or used facial recognition technology, 14 reported using the technology to support criminal investigations. For example, the FBI's Next Generation Identification Interstate Photo System allows users to search a database of over 40 million photos. The system returns a list of potential candidates that law enforcement can use to generate investigative leads. According to the FBI, the system has been used for investigations of violent crimes, credit card and identity fraud, missing persons, and bank robberies, among others.

Six agencies reported using facial recognition technology during May through August 2020 to support criminal investigations related to civil unrest, riots, or protests.⁴ Following the killing of Mr. George Floyd while in the custody of the Minneapolis, Minnesota police department on May 25, 2020, nationwide civil unrest, riots, and protests occurred. Six agencies told us that they used images from these events to conduct facial recognition searches during May through August 2020 in order to assist with criminal investigations (see table 2). All six agencies reported that these searches were on images of individuals suspected of violating the law.

⁴We requested this information from 17 agencies that indicated in their questionnaire response as (1) having a system with facial recognition technology that was in operation, or (2) using another entity's system.

Table 2: Federal Agency Reported Use of Facial Recognition Technology on Images of Individuals Suspected of Violating the Law during Civil Unrest, Riots, or Protests, May through August 2020

Federal Agency	How Agency Reported Using Facial Recognition Technology
Bureau of Alcohol, Tobacco, Firearms and Explosives	In a single instance, used facial recognition technology owned by another law enforcement entity. The search was conducted to help identify an individual suspected of violating the law during the period of civil unrest, riots, or protests.
U.S. Capitol Police	Requested that the Montgomery County Department of Police (Montgomery County, Maryland) conduct facial recognition searches to assist with a criminal investigation. The purpose of the searches was to help identify individuals that confronted and made threats to a member of Congress and the member's spouse outside the White House during the period of civil unrest, riots, or protests.
Federal Bureau of Investigation	Created a digital media tip line and solicited images of people involved in criminal activity during the period of civil unrest, riots, or protests. The agency sought to identify or locate criminal suspects seen in images and video depicting criminal behavior by conducting facial recognition searches using its Next Generation Identification Interstate Photo System.
U.S. Marshals Service	Used a non-government facial recognition service provider to conduct facial recognition searches related to criminal investigations on images from the period of civil unrest, riots, or protests.
U.S. Park Police	Requested that the Maryland National Capital Park Police conduct a facial recognition search using an image from Twitter to identify an individual who allegedly assaulted an officer during the period of civil unrest, riots, or protests. The search was conducted on the National Capital Region Facial Recognition Investigative Leads System. The subject was ultimately charged with Felony Civil Disorder and two counts of Assault on a Police Officer.
U.S. Postal Inspection Service	Used Clearview AI to help identify individuals suspected of criminal activity that took place in conjunction with the period of civil unrest, riots, or protests. This criminal activity included damaging U.S. Postal Service property, stealing mail, opening mail, burglarizing U.S. Postal Service buildings, and committing arson.

Source: GAO analysis of survey data | GAO-21-105309

Three agencies reported using facial recognition technology on images from the U.S. Capitol attack on January 6, 2021.⁵ The three agencies reported using the technology to generate investigative leads for criminal investigations as follows:

- U.S. Capitol Police used Clearview AI to help generate investigative leads. The agency also requested that another federal agency use its system to conduct facial recognition searches on behalf of the U.S. Capitol Police.

⁵We asked agencies whether they used facial recognition on images of the civil unrest, riots, or protests at the U.S. Capitol complex on January 6, 2021. We requested this information from 17 agencies that indicated in their questionnaire response as (1) having a system with facial recognition technology that was in operation, or (2) using another entity's system. See more information on our methodology in appendix I in [GAO-21-518](#). Twelve agencies reported that they did not use the technology for these purposes, three agencies reported using the technology, and two agencies told us they could not answer our questions because the information pertains to ongoing investigations.

- U.S. Customs and Border Protection used its Automated Targeting System to conduct searches at the request of another federal agency.
- Bureau of Diplomatic Security used the Department of State's Integrated Biometric System to conduct searches at the request of another federal agency.

Agencies also reported using facial recognition technology to support other activities, such as surveillance, traveler verification, area access, and research and education. For example, the U.S. Secret Service piloted a system with facial recognition technology to determine whether it could be incorporated into the agency's White House Complex security operations. Specifically, the Secret Service stored photos of 23 volunteer employees within the system. As volunteers moved throughout the White House Complex, their images were captured by closed-circuit television cameras. In real time, the system compared the stored photos to images from the video footage to determine whether they represented the same individual. Secret Service told us it did not plan to implement the system based on the results of the pilot.

Most Agencies Do Not Track Non-Federal Systems in Use or Related Risks

Thirteen agencies do not have complete, up-to-date information on what non-federal systems are used by employees.⁶ These 13 agencies have therefore not fully assessed the potential risks of using these systems, such as risks related to privacy and accuracy. Most federal agencies that reported using non-federal systems did not own systems. Thus, employees were relying on systems owned by other entities, including non-federal entities, to support their operations.

Specifically, we found that 13 of 14 agencies that reported using non-federal systems do not have a mechanism to track what non-federal systems are used by employees (see table 3).⁷ For example, when we requested information from one of the agencies about its use of non-federal systems, agency officials told us they had to poll field division personnel because the information was not maintained by the agency. These agency officials also told us that the field division personnel had to

⁶By complete, up-to-date information, we mean that an agency has ongoing knowledge of what non-federal systems with facial recognition technology are used by employees. By non-federal systems, we are referring to systems owned by state, local, tribal, territorial, and non-government entities.

⁷Fifteen agencies reported using non-federal systems; however, we excluded U.S. Probation and Pretrial Services because it does not use facial recognition technology to support criminal investigations. All 14 agencies discussed in this section reported using the technology to support criminal investigations.

work from their memory about their past use of non-federal systems, and that they could not ensure we were provided comprehensive information about the agency's use of non-federal systems. Officials from another agency initially told us that its employees did not use non-federal systems; however, after conducting a poll, the agency learned that its employees had used a non-federal system to conduct more than 1,000 facial recognition searches.

Table 3: Tracking of Employee Use of Non-Federal Systems with Facial Recognition Technology among Selected Federal Agencies

Federal Agency	Have Mechanism to Track What Non-Federal Systems Are used by Employees
U.S. Immigration and Customs Enforcement	Yes
Bureau of Alcohol, Tobacco, Firearms and Explosives	No
Bureau of Diplomatic Security	No
U.S. Capitol Police	No
U.S. Customs and Border Protection	No
Drug Enforcement Administration	No
Federal Bureau of Investigation	No
U.S. Fish and Wildlife Service	No
Food and Drug Administration, Office of Criminal Investigations	No
Internal Revenue Service, Criminal Investigation Division	No
U.S. Marshals Service	No
U.S. Park Police	No
U.S. Postal Inspection Service	No
U.S. Secret Service	No

Source: GAO analysis of agency information. | GAO-21-105309

Note: Federal agencies marked "No" may have known that employees used certain systems, but they do not have a mechanism to provide complete, up-to-date information of what systems are used by employees.

Numerous risks to federal agencies and the public can accompany the use of facial recognition technology. In particular, these risks can relate to privacy and the accuracy of a system. For example, when agencies use facial recognition technology without first assessing the privacy implications, there is a risk that the agencies will not adhere to privacy-related laws, regulations, and policies. There is also a risk that non-federal system owners will share sensitive information (e.g. photo of a suspect) about an ongoing investigation with the public or others.

Although the accuracy of facial recognition technology has increased dramatically in recent years, risks still exist that searches will provide inaccurate results. For example, if a system is not sufficiently accurate, it could unnecessarily identify innocent people as investigative leads. The system could also miss investigative leads that could otherwise have been revealed. In December 2019, the National Institute of Standards and Technology reported that facial recognition algorithms it tested differed in accuracy widely by race, ethnicity, or country of origin, as well as by gender and age.⁸ Some members of Congress, privacy groups, and others have expressed concerns that facial recognition technology's higher error rates for certain demographics could result in disparate treatment, profiling, or other adverse consequences for members of these populations.

One agency—the U.S. Immigration and Customs Enforcement—reported that it was in the process of implementing a mechanism to track what non-federal systems are used by employees. According to U.S. Immigration and Customs Enforcement officials, in November 2020 they were in the process of developing a list of approved facial recognition technologies that employees can use. In addition, log-in sheets will be made available to employees, allowing supervisors to monitor employee use of the technologies. The agency also assessed privacy and accuracy risks associated with its use of facial recognition technology, including non-federal systems.⁹

However, 13 federal agencies cannot fully assess the risks of using non-federal systems because they do not have complete, up-to-date information on what systems are actually used by employees. Therefore, in June 2021 we recommended that these 13 agencies: (1) implement a mechanism to track what non-federal systems with facial recognition technology are used by employees to support investigative activities; and (2) after implementing a mechanism to track non-federal systems, assess

⁸National Institute of Standards and Technology, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NIST Interagency or Internal Report 8280 (Dec. 19, 2019). The National Institute of Standards and Technology reported that it tested 189 mostly commercial algorithms from 99 developers and that performance differences varied by the algorithms tested, with some performing better than others. For a small number of the one-to-many algorithms, differences in false positives across demographic groups were undetectable. The extent of performance differences varied by the developer, type of error, and quality of the facial images.

⁹Department of Homeland Security, Privacy Impact Assessment for the ICE Use of Facial Recognition Services, DHS/ICE/PIA-054 (May 13, 2020).

the risks of using such systems, including privacy and accuracy-related risks.¹⁰

These agencies generally concurred with our recommendations.¹¹ We believe that expeditious implementation of our recommendations is essential. By implementing a mechanism to track what non-federal systems are used by employees, agencies will have better visibility into the technologies they rely upon to conduct criminal investigations. In addition, by assessing the risks of using these systems, including privacy and accuracy-related risks, agencies will be better positioned to mitigate any risks to themselves and the public.

Chair Jackson Lee, Ranking Member Biggs, and Members of the Subcommittee, this concludes my prepared statement. I would be pleased to respond to any questions you may have at this time.

GAO Contact and Staff Acknowledgements

If you or your staff have any questions about this testimony, please contact Gretta L. Goodwin, Director, Homeland Security and Justice, at (202) 512-8777 or GoodwinG@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Jeffrey Fiore (Assistant Director), Andrea Bivens (Analyst-In-Charge), Jennifer Beddor, Emily Flores, Richard Hung, Jason Jackson, Heidi Nielson, Erin Pineda, and Adam Schrier. Key contributors for the previous work that this testimony is based on are listed in the previously issued product.

¹⁰We made these recommendations to all 13 agencies that reported "No" in table 3 above.

¹¹As of June 2021, the 13 federal agencies have not implemented these recommendations.

Appendix I: Federal Agencies That Participated in GAO's Survey Questionnaire on Facial Recognition Technology

Our June 2021 report included the results of a survey questionnaire we sent to 42 federal agencies that employed law enforcement officers.¹ The survey focused on agency ownership and use of facial recognition technology. See the list of 42 federal agencies in table 4 below.

Table 4: Federal Agencies That Participated in GAO's Survey Questionnaire on Facial Recognition Technology

Federal Agency	Department
Forest Service	Agriculture
Bureau of Industry and Security	Commerce
National Oceanic and Atmospheric Administration, Office of Law Enforcement	Commerce
Office of Security	Commerce
Secretary's Protective Detail	Commerce
Pentagon Force Protection Agency	Defense
National Nuclear Security Administration	Energy
Food and Drug Administration, Office of Criminal Investigations	Health and Human Services
National Institutes of Health, Division of Police	Health and Human Services
U.S. Customs and Border Protection	Homeland Security
Federal Emergency Management Agency, Mount Weather Police	Homeland Security
Federal Protective Service	Homeland Security
U.S. Immigration and Customs Enforcement	Homeland Security
Office of the Chief Security Officer	Homeland Security
U.S. Secret Service	Homeland Security
Transportation Security Administration	Homeland Security
Bureau of Indian Affairs, Office of Justice Services	Interior
Bureau of Land Management	Interior
Bureau of Reclamation	Interior
U.S. Fish and Wildlife Service	Interior
U.S. Park Police	Interior
National Park Service Rangers	Interior
Bureau of Alcohol, Tobacco, Firearms, and Explosives	Justice
Drug Enforcement Administration	Justice
Federal Bureau of Investigation	Justice
Federal Bureau of Prisons	Justice

¹GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, [GAO-21-518](#) (Washington D.C.: June 3, 2021). In our June 2021 report, we defined federal law enforcement officers as full-time employees with federal arrest authority and who are authorized to carry firearms while on duty. See more information on our scope and methodology in our June 2021 report.

**Appendix I: Federal Agencies That Participated
in GAO's Survey Questionnaire on Facial
Recognition Technology**

Federal Agency	Department
U.S. Marshals Service	Justice
Division of Protective Operations	Labor
Bureau of Diplomatic Security	State
Bureau of Engraving and Printing Police	Treasury
Internal Revenue Service, Criminal Investigation Division	Treasury
U.S. Mint Police	Treasury
Police Service	Veterans Affairs
Amtrak Police Department	—
Environmental Protection Agency, Criminal Investigation Division	—
National Aeronautics and Space Administration, Office of Protective Services	—
U.S. Postal Inspection Service	—
Smithsonian Institution, Office of Protection Services	—
Tennessee Valley Authority Police	—
Administrative Office of the U.S. Courts, U.S. Probation and Pretrial Services	—
U.S. Capitol Police	—
Government Publishing Office, Uniform Police Branch	—

Legend: — Not Applicable

Source: GAO information. | GAO-21-105309

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on Facebook , Flickr , Twitter , and YouTube . Subscribe to our RSS Feeds or Email Updates . Listen to our Podcasts . Visit GAO on the web at https://www.gao.gov .
To Report Fraud, Waste, and Abuse in Federal Programs	Contact FraudNet: Website: https://www.gao.gov/about/what-gao-does/fraudnet Automated answering system: (800) 424-5454 or (202) 512-7700
Congressional Relations	Orice Williams Brown, Managing Director, WilliamsO@gao.gov , (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov , (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548
Strategic Planning and External Liaison	Stephen J. Sanford, Managing Director, spel@gao.gov , (202) 512-4707 U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548



Please Print on Recycled Paper.

Ms. JACKSON LEE. I will, Mr. Lee, come to you for a broad question on civil rights. Let me ask, Dr. Alexander, 18,000 police departments, one of the reasons why NOBLE has been so instrumental in helping us push for the George Floyd Justice in Policing Act to find regular order that will help police, not diminish police. How do you respond to the idea—also, to my Members believe that we should have a follow-up hearing with some of our Federal law enforcement representatives that were cited by this excellent report that Dr. Goodwin has put forth through the GAO, and that may be in a classified manner, but we will be presenting that in the future.

Dr. Alexander, to note that it was determined through the Federal system that employees were using the system without their hierarchy knowing, what do you think that means for the 18,000 police departments where this kind of technology comes into their possession and how that relates to your point about police community relationships, but also victims, and I'm going to call him a victim, and I hope that he can made whole, and that is Mr. Williams and his family.

Dr. Alexander.

Dr. ALEXANDER. Thank you, Madam Chair.

Yes, there's 18,000 police departments in this country, and oftentimes, we are finding more and more we have got 18,000 different ways things are being done and how they are being responded to, how they are being disciplined, how they are being managed, how they are being trained, et cetera. When you have one organization—and all it takes is just one, quite frankly, in the eyes of the American public—they all see policing as the same. It doesn't make it right, but that is the reality of it. If I do something well as a police officer, we all jump up and down and say, hey. If I do something horrible, we all have to take that hit, too.

To your question, I think it becomes important to recognize that appropriate training is going to have to be regulated at a Federal level, and there's going to have to be some Federal standard, I truly believe, the same way we do with fingerprint, and with DNA, and with other forensic methods that have proven to be of value in the law enforcement and public safety community, because the whole idea about this particular piece of technology is that it is very convoluted, and it's very complicated, and there are going to be cases that are going to go before the courts that we haven't even thought about yet as it relates to this technology, still yet to be examined.

So, I just think, Congresswoman, that due diligence will be given to these local agencies across this country. If they have an opportunity to be well-trained, there would be the standardization to the utilization of this technology, there would be ongoing certification, there would be practices that are held to the highest standards of science. In addition to that, I think it becomes important as well that the public understands what facial recognition technology is, because we have talked about it a lot within the context of policing, and within Congress, but a lot of people in our communities across this country don't understand exactly what it means, and when they do hear about the cases, they hear about the cases that are often associated with that of Mr. Williams.

Ms. JACKSON LEE. I would think minimally that—and you don't have to answer. I'm just going to make this based upon your response—minimally, that police departments need to be aware of when the technology is in their possession, and whether or not it's a detective with sloppy work, that that is being used and the individuals given the authority to use it are well-trained and, as you indicated, certified.

I would just like to place that on the record because the title of the GAO report said that our Federal agencies should have a better awareness of these systems being used by employees. That is actually shocking and amazing to me, and I think that can be parlayed out into the field with the other 18,000 police departments.

Thank you for your answer.

I indicated that my concern has been the unreasonable search and seizure. I would like both Professor Laurin and, as well—and I think this was raised by one of our Members, but I would like maybe a succinct answer from both of you, Professor Laurin, with your academic background, you focused on criminal procedure. I don't think that we are without tools. We have the ability on the Judiciary Committee to look at the Federal criminal procedure as we do civil procedure.

In any event, Mr. Tolman, as a former U.S. Attorney, in cases where an investigation results in prosecution, should prosecutors be required to inform the defendant that facial recognition technology was used to identify them in any part of the process? Obviously, it is investigative, and should alternate positive matches be required to be produced as that investigation goes forward and if it ultimately comes into court? I know that one of our Members mentioned the Brady defense, but how should we respond to that? Professor Laurin first, and then Mr. Tolman.

Ms. LAURIN. Thank you, Chair.

My bottom line view is it's absolutely right, the observation that with respect to Federal criminal procedure there's some very direct interventions that Congress can make, and while I think the scope of Rule 16, frankly, is always sort of a fraught discussion, I think there are important limited interventions that can be made in terms of requiring access to facial recognition, to the fact of the search, to alternative matches, to information on confidence levels.

Again, as I said, I think to the extent possible, it's really essential that the defense have access to the algorithms to what's inside the Black box to be able to evaluate the reliability of the technology. That could all be a matter of sort of statutory change without having to worry about the courts sorting through the morass of whether Brady Doctrine encompasses that.

Ms. JACKSON LEE. Thank you.

Mr. TOLMAN. I would simply add that—

Ms. JACKSON LEE. Thank you. Yes, Mr. Tolman.

Mr. TOLMAN. The Professor is absolutely correct. I agree with everything she just articulated.

I would add that, unlike a lineup where a prosecutor is required to hand over alternative individuals that might have been placed in the lineup, and the rationale for the lineup that was utilized, facial recognition technology requires the prosecutor, and should require the prosecutor to turn over more if the intention is to give

the defense counsel all that it needs to assess the reliability and the admissibility of such evidence.

So, we are at a new ball game with this technology, and it will require more to be given from a prosecutor to a defense attorney under the strictures of our constitutional protections.

Ms. JACKSON LEE. I think that—

Ms. LAURIN. I would just add one additional note, which is that it is essential that timing be addressed because if defense counsel is only able to access this on the eve of trial, it does no good in terms of evaluating whether a guilty plea is an appropriate resolution. It does no good in terms of preparing to challenge the admissibility of evidence, and so early discovery is important as well.

Ms. JACKSON LEE. Early discovery and early knowledge? Is that my understanding?

Ms. LAURIN. [Nonverbal response.]

Ms. JACKSON LEE. Thank you so much.

Professor Friedman, I just wanted to clarify, when you said “regulation,” in what framework are you speaking?

Mr. FRIEDMAN. So, you know, I think what’s important here is comprehensive regulation. That does two general things: One is regulate the technology as best as we understand it right now, so we know that there are very serious problems with the technology, and they need to be addressed. Then the other is, there’s a lot we need to learn.

So, one of the things that Congress could do immediately is instruct some entity, like NIST, to actually test the technology under operational conditions, how law enforcement is using it, because there are very, very serious concerns about accuracy and bias, particularly racial bias, and we get numbers reported, but those numbers bear no reflection to how law enforcement is actually using the technology, and what little we know from this suggests that those error rates may be quite high as others have indicated.

So, there’s a list of things that I think we should—that Congress should have this study, and then I think there’s a list of immediate safeguards we could put in place, for example, best-practice protocols about what it means to have a human in the loop that verifies what the algorithm does.

Ms. JACKSON LEE. Thank you very much.

Ms. Frederick—and I’m going to finish with Mr. Lee. Ms. Frederick, you have been keen on the providers, or the tech entities that control this technology. From your perspective, what would be a regulation in that entity, in that arena?

Ms. FREDERICK. Well, ma’am, as you know, I work for the Heritage Foundation, and we are about limited government, and we do not really support regulation when it comes to—or robust regulation when it comes to private entities. So, my solution would be, we have to encourage the programs within these companies, the leaders in these companies to institute those privacy-by-design mechanisms, so make sure in the design phase of creating an algorithm, you are in viewing it with privacy protections, and that is why I sort of harken to the differential privacy. We have methods of encryption that are getting more and more powerful and much better, decentralized models of data storage, studying models of machinery.

So, if we as—or excuse me, if you as Congress can sort of impress upon these companies that they need to build in these data privacy protections, I think that is a good start point, short of actual regulation on private companies.

Ms. JACKSON LEE. Well, in the spirit of my Ranking Member, you know this is a bipartisan hearing, so we wanted to make sure we welcomed your thoughts as well, which will be very helpful to us.

Let me have Mr. Williams, and then, Mr. Lee, you will have the last word. Mr. Williams, I think you have heard from all of us. We are appalled at what happened to you. We are stunned. We know that there are good intentions. I will be introducing some articles where this technology was used.

We also heard from Dr. Alexander that there is good policing out there working to do positive things. In your instance, you fell into a very bad trap. What do you want to leave us with as a victim, not a victim in your own self, but a victim of this technology that should not have happened? Again, I started out by apologizing to you and your family, and we will be eagerly watching your lawsuit possibly pursued by the ACLU, if I'm correct. What do you want us to know as you end your testimony here?

You need to unmute.

Mr. WILLIAMS. Yes, I will unmute. Thank you.

First, I just want to say thank you for inviting me to come tell my story, and I hope that going forward, we can figure out a way to, like they say, to regulate because it's already being used, so we need to get it fixed so that it works more in a way that it works properly, I should say, because in the current state, it's wrong. They get it wrong even when they get it right, and I don't know if that makes sense.

Like, you don't have a—you really don't have a say—so, I mean, throughout the time that nobody has ever signed up to say, hey, use my picture from my ID in your mug book. Like I said a little earlier, they didn't even use my current driver's license. They used one previous from when, I guess, I might have looked younger at that point. I don't know. I guess all your information is in the system, so it's available to be used.

I was asked a few times about how my daughter took it, and I don't know what the lasting effect is on them. All I know is that at this point, she is upset. Every time we look at her, she—so, I don't know. I'm just—I hate to say I'm thankful that it was a felony larceny, but it just—what if the crime was capital murder or something like that, and then they just came to my house and arrested me? I don't know if I would have got a bond to get out and be free to even talk to you at this point, because the court system is backed up that they probably wouldn't have even got to me yet, and I would still be locked up for something I didn't do. All right.

I kind of cringe to think about it like that, because I did not get to say anything. I didn't have any rights read to me or anything. They showed up, asked me my name, and I asked for a warrant. They didn't just bring one. I mean, I resisted arrest, but I was in my driveway, and I'm, like, "what are you all doing?" He was, like, "Are you Robert Williams?" He was, like, "all right you are under arrest." I'm, like, "for what?" He was, like, "I can't tell you." I'm, like, you can't even tell me what I'm under arrest for, but I'm

under arrest. They took me immediately down to the detention center, and I got fingerprinted and mug-shotted right then and there, and I assumed that my fingerprints were clear and I would be out, and that didn't mean anything. It didn't mean—if my fingerprints went in, so what?

All right. Now, they have a mug shot to add to it. It was so backwards if that makes sense, right? I just feel like I'm just a regular, and I thought I knew the law, but I was wrong. So, hopefully we get some change.

Ms. JACKSON LEE. That is powerful, Mr. Williams. You are seeking—I would just simply say you are seeking justice.

Mr. WILLIAMS. Yes, ma'am.

Ms. JACKSON LEE. You deserve it, you really do.

Mr. Lee, you obviously represented sort of a family of those who have been fighting these issues dealing with justice in the criminal justice system, and, so, having listened to Mr. Williams and—I know the position of a ban and a moratorium, but just, if you would, end us on the enormity of the problem, if we are to have facial recognition used randomly in this massive hierarchy of 18,000 police departments without some intervention. It may be your form. It may not be. What can happen to persons who wind up like Mr. Williams?

I'm shocked that you can't get a reason why you are being arrested. I thought you were entitled to that. To use facial recognition, the people that he was in the lineup with didn't look like him. It didn't look like him when they put the picture up to him. So, how is that just an undermining of civil rights and civil liberties in this country, if used as it seemed to have been used with Mr. Williams?

Mr. LEE. Madam Chair—

Ms. JACKSON LEE. Please, Mr. Lee.

Mr. LEE. Yes, Madam Chair. I think there's a broader context of policing that we must keep in mind that is especially instructive when talking about the case of Mr. Williams. Also, why so many—the Leadership Conference and its coalition organization support a ban, moratorium, and, Ms. Frederick, I'm going to steal tactical pause from you here on out in my policy conversations. It's because we can't separate the tools from the context of the American policing system. We have evidence of that system over decades, centuries of how Black bodies, and disproportionately Black people are treated within the criminal legal justice system.

We can't separate those tools. Then if you add the whole history of that criminal legal system to a tool that is known in the best of conditions to be biased against Black people and against women and misclassifies or misidentifies Members of the LGBTQ-plus community, people with disabilities, right, so many Members of the community that we need to protect because of their protected status and the history of harms that have been done onto their bodies throughout centuries, then we need to have a real conversation about whether this technology actually works the way that we think it does. It doesn't. That has been proved time and time again, whether the National Institute of Standards and Technology, whether the research by Joy Buolamwini and Timnit Gebru, right, whether we are talking about the ACLU's use of the Amazon facial

recognition technology to identify even Members of Congress who are public figures.

It's being used in communities that are already over-policed and over-surveilled, and it is the least likely to work for those exact same communities, and the community is not involved in the process. There's no public airing of widespread use. Congress has not been—Congress has not been asked, or Congress has not legislated on these topics.

Then there's even opacity with which the tech is used that is compounded by the opacity of policing practices in general, and law enforcement agencies. We don't know still, even with the GAO report, how deep law enforcement is using facial recognition technology, nor the full extent of those technologies' writ large.

Community engagement is not a check box. It's a continuous conversation, and no one knows. There are secret hearings. There are classified briefings. The public does not know the full extent of facial recognition technology, and really broadly, digital evidence capacity of law enforcement capacity writ large.

We will continue to consistently call for a moratorium or ban on these technologies, and we would be more than happy to work with this Committee and Congress to imagine a solution and imagine a world of policing that puts the civil rights and civil liberties of marginalized communities first, not last, and not using these same communities as basically test cases when these technologies do not work.

Ms. JACKSON LEE. Okay. Thank you so very much. Thank you so very much.

Thank you to each of the Witnesses for their profound testimony, and thank you to my Members, or the Members of this Committee. Mr. Biggs, as Ranking Member, thank you for joining me on, I believe, a hearing that will be very constructive going forward as evidenced by the questions and the responses and, of course, the expert Witnesses that we had today.

So, this concludes today's hearing.

Before I conclude, I would like to submit into the record: Center for Strategic and International Studies, "The Problem of Bias in Facial Recognition," May 1, 2020; Washington Post article, "How America's Surveillance Networks Helped the FBI Catch the Capitol Mob," and that is dated April 2, 2021; and then The Washington Post responding to the "Federal study confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanded Use," December 19, 2021. I want those articles submitted into the record.

[The information follows:]

MS. JACKSON LEE FOR THE RECORD

Photo: DAVID MCNEW/AFP via Getty Images

BLOG POST - STRATEGIC TECHNOLOGIES BLOG
<<https://www.csis.org/blogs/strategic-technologies-blog>>

SHARE

The Problem of Bias in Facial Recognition

May 1, 2020

By: William Crumpler

Researchers have found that leading facial recognition algorithms have different accuracy rates for different demographic groups. The first study to demonstrate this result was a 2003 report
<<https://nvlpubs.nist.gov/nistpubs/legacy/ir/nistir6965.pdf>> by the National Institute of

Standards and Technology (NIST), which found that female subjects were more difficult for algorithms to recognize than male subjects, and young subjects more difficult to recognize than older subjects. In 2018, researchers from MIT and Microsoft generated news with a report <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf> showing that gender classification algorithms—which are related, though distinct from face identification algorithms—had error rates of just 1% for white men, but almost 35% for dark-skinned women. The most thorough investigation of this disparity was completed by NIST in 2019. Through their testing, NIST confirmed <https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf> that a majority of algorithms exhibit demographic differences in both false negative rates (rejecting a correct match) and false positive rates (matching to the wrong person).

NIST found that demographic factors had a much larger effect on false positive rates—where differences in the error rate between demographic groups could vary by a factor of ten or even one hundred—than false negative rates—where differences were generally within a factor of three. Differences in false positive rates are generally of greater concern, as there is usually greater risk in misidentifying someone than in having someone be incorrectly rejected by a facial recognition system (as when your iPhone doesn't log you in on the first try). NIST found that Asians, African Americans, and American Indians generally had higher false positive error rates than white individuals, women had higher false positive rates than men, and children and the elderly had higher false positive rates than middle aged adults.

However, NIST also came to several encouraging conclusions. The first

is that differences between demographic groups were far lower in algorithms that were more accurate overall. This means that as facial recognition systems continue to improve <https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%e2%80%93-and-why-does-it-matter>, the effects of bias will be reduced. Even more promising was that some algorithms demonstrated no discernible bias whatsoever, indicating that bias can be eliminated entirely with the right algorithms and development processes. The most important factor in reducing bias appears to be the selection of training data used to build algorithmic models. If algorithms are trained on datasets that contain very few examples of a particular demographic group, the resulting model will be worse at accurately recognizing members of that group in real world deployments. NIST's researchers theorized that this may be the reason many algorithms developed in the United States performed worse on Asian faces than algorithms developed in China. Chinese teams likely used training datasets with greater representation of Asian faces, improving their performance on that group.

Because of the importance of training data selection on the performance and bias of facial recognition algorithms, these datasets have become an increasingly popular target for regulatory proposals. The EU, for example, recently proposed

https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf that a regulatory framework for high-risk AI systems like facial recognition include requirements that training data be “sufficiently broad,” and reflect “all relevant dimensions of gender, ethnicity and other possible grounds of prohibited discrimination.” Training data audits to confirm the quality of training datasets could become an

important tool for addressing the risks of bias in facial recognition. However, an expanded audit regime could face resistance from developers who will oppose adding additional time or cost to the development process, or opening any part of their algorithm to third party investigation.

Government action will be necessary to encourage the adoption of training data audit practices. The easiest first step would be to update procurement policies at the state, local, and federal level to ban government purchases from facial recognition vendors that have not passed an algorithmic audit incorporating the evaluation of training data for bias. These audits could be undertaken by a regulator or by independent assessors accredited by a government. At a minimum, this should be required by law or policy for high-risk uses like law enforcement deployments. Federal policymakers could also help to reduce bias risks by empowering NIST to oversee the construction of public, demographically representative datasets that any facial recognition company could use for training.

However, bias can manifest not only in the algorithms being used, but also in the watchlists these systems are matching against. Even if an algorithm shows no difference in its accuracy between demographics, its use could still result in a disparate impact if certain groups are over-represented in databases. African American males, for example, are disproportionately represented in the mugshot databases many law enforcement facial recognition systems use for matching. This is the result of larger social trends, but if facial recognition becomes a common policing tool, this could mean that African American males

will be more frequently identified and tracked since many are already enrolled in law enforcement databases. Unlike the question of differential accuracy, this is not a problem that can be solved with better technology.

This highlights the importance of shifting the conversation around the risks of facial recognition. Increasingly, the primary risks will not come from instances where the technology fails, but rather from instances where the technology works exactly as it is meant to. Continued improvements to technology and training data will slowly eliminate the existing biases of algorithms, reducing many of the technology's current risks and expanding the benefits that can be gained from responsible use. But this will also make deployments more attractive to operators, creating new sets of concerns. As policymakers consider how best to construct governance systems to manage facial recognition, they should ensure their solutions are tailored to where the technology is heading, not where it is at today. Bias in facial recognition algorithms is a problem with more than one dimension. Technical improvements are already helping contribute to the solution, but much will continue to depend on the decisions we make about how the technology is used and governed.

William Crumpler is a research assistant with the Technology Policy Program at the Center for Strategic and International Studies in Washington, DC.

The Technology Policy Blog is produced by the Technology Policy Program at the Center for Strategic and International Studies (CSIS),

a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

📧 MEDIA QUERIES

Contact H. Andrew Schwartz
Chief Communications Officer
Tel: 202.775.3242

Contact Paige Montfort
Media Relations Coordinator, External Relations
Tel: 202.775.3173

RELATED

Cybersecurity and Technology <<https://www.csis.org/topics/cybersecurity-and-technology>>, Emerging Technologies <<https://www.csis.org/programs/strategic-technologies-program/archives/emerging-technologies>>, Strategic Technologies Program <<https://www.csis.org/programs/strategic-technologies-program>>, Technology and Innovation <<https://www.csis.org/topics/cybersecurity-and-technology/technology-and-innovation>>

MORE FROM THIS BLOG

BLOG POST

BLOG POST

How America's surveillance networks helped the FBI catch the Capitol mob

Federal documents detailing the attacks at the U.S. Capitol show a mix of FBI techniques, from license plate readers to facial recognition, that helped identify rioters. Digital rights activists say the invasive technology can infringe on our privacy.

By [Drew Harwell](#) and [Craig Timberg](#)
April 2, 2021 at 9:00 a.m. EDT

Debra Maimone pulled down her American flag mask for a moment on Jan. 6 and gazed at the unruly mob of supporters of President Donald Trump overrunning the U.S. Capitol.

"Put your mask on," warned her fiancé, as the couple stood beneath an unblinking array of surveillance cameras. "I don't want them to see you."

It was too late.

That scene, recorded in a cellphone video Maimone posted to the social media site Parler, helped FBI agents identify the Pittsburgh-area couple and pinpoint their location inside the Capitol, FBI agents said in a federal [criminal complaint](#) filed before Maimone's arrest last month.

Video cameras mounted throughout the complex also captured the pair from 10 different angles, the complaint says, as they allegedly stormed the halls of Congress, rummaged through a police bag and made off with protective equipment that Senate officials kept on hand in case of a chemical attack.

Their case is among more than 1,000 pages of arrest records, FBI affidavits and search warrants reviewed by The Washington Post detailing one of the biggest criminal investigations in American history. More than 300 suspects have been charged in the melee that shook the nation's capital and left five people dead.

The federal documents provide a rare view of the ways investigators exploit the digital fingerprints nearly everyone leaves behind in an era of pervasive surveillance and constant online connection. They illustrate the power law enforcement now has to hunt down suspects by studying the contours of faces, the movements of vehicles and even conversations with friends and spouses.

But civil liberties groups warn that some of these technologies threaten Americans' privacy rights. More than a dozen U.S. cities have banned local police or government officials from using facial recognition technology, and license plate readers have sparked lawsuits arguing that it is unconstitutional to constantly log people's locations for government review, with scant public oversight.

"Whenever you see this technology used on someone you don't like, remember it's also being used on a social movement you support," said Evan Greer, director of the digital rights advocacy group [Fight for the Future](#). "Once in a while, this technology gets used on really bad people doing really bad stuff. But the rest of the time it's being used on all of us, in ways that are profoundly chilling for freedom of expression."

The cache of federal documents lays out a sprawling mix of FBI techniques: license plate readers that captured suspects' cars on the way to Washington; cell-tower location records that chronicled their movements through the Capitol complex; facial recognition searches that matched images to suspects' driver's licenses or social media profiles; and a remarkably deep catalogue of video from surveillance systems, live streams, news reports and cameras worn by the police who swarmed the Capitol that day.

Agents in nearly all of the FBI's 56 field offices have executed at least 900 search warrants in all 50 states and D.C., many of them for data held by the telecommunications and technology giants whose services underpin most people's digital lives. The responses supplied potentially incriminating details about the locations, online statements and identities of hundreds of suspects in an investigation the Justice Department called in a [court motion](#) last month "one of the largest in American history, both in terms of the number of defendants prosecuted and the nature and volume of the evidence."

"If the event happened 20 years ago, it would have been 100 times harder to identify these people," said Chuck Wexler, executive director of the [Police Executive Research Forum](#), a D.C.-based think tank. "But today it's almost impossible not to leave your footprints somewhere."

The federal documents cite evidence gleaned from virtually every major social media service: Parler is mentioned in more than 20 cases, Twitter in more than 60 and Facebook in more than 125. On Snapchat, a woman posted videos "bragging about the attack," according to one criminal complaint. In another, a man was said to have posted video to TikTok of himself fighting with National Guard members and getting pepper-sprayed.

In at least 17 cases, the federal documents cite records from telecommunications giants AT&T, Verizon or T-Mobile, typically after serving search warrants for a range of subscriber data, including cellphone locations.

Investigators also sent "geofence" search warrants to Google, asking for the account information of any smartphone Google had detected on Jan. 6 inside the Capitol via GPS satellites, Bluetooth beacons and WiFi access points. Investigators then compiled an "exclusion list" of phones owned by people who were authorized to be in the Capitol on Jan. 6, including members of Congress and first responders. Everyone else was fair game.

Federal officials filed similarly broad search warrants to Facebook, demanding the account information associated with every live stream that day from inside the vast complex.

One warrant targeting Brandon Miller, an Ohio man who wrote on Facebook that he had traveled to Washington to "witness history," yielded his Facebook posts, credit card information, phone number and home Zip code, giving FBI agents the clues necessary to later match his photo to Capitol surveillance camera footage and his Ohio driver's license.

When Miller was asked on Facebook the day after the riots whether he and his wife, Stephanie, had gotten into trouble, he had written back, "No not yet anyway lol," a [criminal complaint](#) shows.

But data from a Google search warrant allowed FBI agents to map the exact locations of their phones that day — from the point where rioters smashed into the Senate chamber, to the speaker's office in the heart of the Capitol, according to the [complaint](#). Another search warrant to their cellular carrier, AT&T, added additional information about their whereabouts, plus their names and home address. Stephanie Miller's attorney declined to comment, and Brandon Miller's attorney did not respond to requests for comment.

License plate readers and facial recognition software together played a documented role in helping identify suspects in nearly a dozen cases, the federal records show. In many cases, agents used existing government contracts to access privately maintained databases that required no court approval. In several cases, including for facial recognition searches, it's unclear what software the government used to build the cases for arrests.

The FBI declined to comment for this story. The incidents described remain allegations, with none of the cited cases having been adjudicated yet. In most cases, suspects' attorneys have not yet filed defenses against charges that in many instances are only a few weeks old, court records show.

Many cases also hinge on imperfect technology and fallible digital evidence that could undermine prosecutors' claims. Blurry license plate reader images, imprecise location tracking systems, misunderstood social media posts and misidentified facial recognition matches all could muddy an investigation or falsely implicate an innocent person.

Fruitless efforts to hide

Many of the Trump supporters who marauded through the Capitol that day showed little interest in concealing their presence, posting selfies, gloating on Twitter and sharing video of chaotic violence and ransacked hallways. James Bonet, of Upstate New York, uploaded a Facebook video of himself inside the Capitol's halls, allegedly smoking a joint, a [criminal complaint](#) states. And Dona Bissey, an Indiana follower of the extremist ideology QAnon, posted a location-tagged photo of herself and her friends to a publicly available Facebook page: "Picking glass out of my purse," she wrote, according to a [charging document](#). "Best f---ing day ever!!"

Others, however, attempted to hide their identities and throw off investigators afterward, according to FBI agents' claims. Suspects covered their faces, switched hats during the day and threatened family members and witnesses to keep quiet afterward, the criminal complaints allege. They deleted social media accounts, hid out in hotels or ditched potentially incriminating phones, according to the documents. One suspect stopped using a car he feared might be on authorities' radar, the federal documents show, while another said he "fried" his electronics in a microwave. The FBI's surveillance efforts found them anyway.

One man from New York's Hudson Valley, William Vogel, had his round-trip voyage to D.C. photographed by license plate readers at least nine times on Jan. 6, from the Henry Hudson Bridge in the Bronx at 6:06:08 that morning to Baltimore's Harbor Tunnel Thruway at 9:15:27 a.m. and back to the George Washington Bridge in Fort Lee, N.J., at 11:59:22 that night, a [criminal complaint](#) claims.

Vogel generated more evidence of his presence inside the Capitol with a set of videos he posted to Snapchat, the complaint said. And though no license plate scanners captured his car in D.C., they offered other clues to his movement: A photo that morning from a stretch of Interstate 95 northeast of Baltimore showed a comically oversized "Make America Great Again" hat on Vogel's dashboard. Agents said in the complaint that they later matched it to a Facebook selfie in which he appeared to be wearing "the same large red hat."

Installed on thousands of streetlights, speed cameras, toll booths, police cars and tow trucks across the United States, the scanners record every passing vehicle into databases run by contractors such as Vigilant Systems, which reports that it has recorded 5 billion license plate locations nationwide. In Maryland alone, government and police scanners captured more than 500 million plates last year, state data shows.

Dominick Madden, a New York City sanitation worker who was on sick leave when he allegedly stormed the Capitol, had his car's license plate scanned half a dozen times in his round-trip journey to Washington, a criminal complaint states. Madden was also allegedly caught on video walking through the Capitol's Senate wing in a blue QAnon sweatshirt. He has pleaded not guilty, and his attorney did not respond to requests for comment.

In many cases, the documents quote suspects expressing confidence that they had slipped beyond the FBI's grasp. When an unnamed Parler user warned Maimone — the Pittsburgh-area woman with the American flag mask — that authorities would be arresting anyone who entered the Capitol building illegally on Jan. 6, she dismissed the idea through her account, “TrumpIsYourPresident1776.”

“Lmao yaaaaaaaaa sure thing buddy!” she wrote in an exchange cited in the criminal complaint charging Maimone with theft, violent entry and disorderly conduct on Capitol grounds. A D.C. judge signed a warrant for her arrest last month.

FBI agents got help identifying Maimone and her fiancé, Philip Vogel (no known relation to William Vogel), by manually comparing his voice and hand tattoos to a Pittsburgh TV news report from last year, during which he talked of being rescued one night after his fishing boat hit a log and capsized, the federal complaint said.

Investigators also matched Vogel's gray beanie to a photo he and Maimone had posted to the Yelp profile of their contracting business, according to the complaint. And they matched his scarf to one he'd worn in a selfie posted to his Facebook account in which he celebrated catching a “monster” fish in the Potomac River one day after the riot.

Attorneys for Maimone and Vogel declined to comment. The couple have been released from custody after they each paid \$10,000 in bond and agreed to “stay away from D.C.,” court records show.

Other alleged insurrectionists ended up helping investigators even as they attempted to cover their tracks, FBI agents wrote in charging documents. One man entered the Capitol wearing a dark cowboy hat and a large respirator that covered all but his eyes and forehead. But he also took a selfie beneath a marble statue of the nation's seventh vice president, John C. Calhoun, a fixture of the large “crypt” room beneath the Capitol Rotunda. A tipster who received the photo forwarded it to the FBI, a criminal complaint said, along with a suggested name: Andrew Hatley.

Hatley denied participating in the attack, writing on Facebook: “It has come to my attention that there was someone who looks like me at the Capitol. I'd like to set the record straight. I don't have that kind of motivation for lost causes. I just don't care enough anymore, certainly not enough for all that.”

But he allegedly left evidence to the contrary in the logs of a social media app, Life360, often used by family members to keep track of each other. When a tipster told FBI agents that Hatley had the app on his smartphone, they sent a search warrant to Life360 days after the attack. Investigators said in the complaint that they then plotted Hatley's travels on “an electronic map of Washington, D.C.” based on the company's logs.

In the just-the-facts style of FBI documents, investigators alleged the evidence erased any doubts: “The data confirms that HATLEY's cellular telephone was at the U.S. Capitol Building during the events described above on January 6, 2021.” Hatley's attorney and Life360 declined to comment.

In another case, an FBI agent wrote in a [criminal affidavit](#) that a “self-professed white supremacist” from Maryland, Bryan Betancur, had asked his probation officer for permission to leave the state on Jan. 6 to hand out Bibles in D.C. with an evangelical group. But Betancur’s court-ordered ankle monitor gave him away, the affidavit claimed, by posting his minute-by-minute location — from Trump’s rally at the White House Ellipse to the Capitol’s steps — to a website investigators could track in real time. He was arrested on Jan. 17, nine days after he told his probation officer he believed the FBI was watching him.

Attorneys for Bissey and William Vogel declined to comment. Attorneys for Betancur and Bonet did not respond to requests for comment.

1 phone, 12,000 pages of evidence

The documents highlight just how much digital evidence an ordinary person sheds in everyday life: In one case, prosecutors said they gathered more than 12,000 pages of data from a suspect’s phone using [Cellebrite](#), a tool popular with law enforcement for its ability to penetrate locked phones and copy their contents. The search also recovered 2,600 pages of Facebook records and 800 cellphone photos and videos.

The FBI said it tracked down suspected rioters who had tried unsuccessfully to evade prosecution. In an [affidavit](#) supporting a search warrant application, an FBI agent said that a relative of Zachary Alam had told investigators he could be seen in video bashing some glass inside the Capitol with his helmet and that he was on the run with no intention of turning himself in. Agents got a D.C. judge to issue a “ping order” for his cellphone, which had been registered with T-Mobile under the name of Superman’s alter ego, Clark Kent, the affidavit said. That ping order allegedly pinpointed Alam’s location to Room 17 of the Penn Amish Motel in rural Pennsylvania. FBI agents arrested him there the next day.

Apple also gave investigators details of Alam’s iCloud account, including his home address, log-in information and the registration dates for his iPhone 7 and MacBook Air, the affidavit said. The tech giant was cited in several cases where agents seized suspects’ iPhones, but no document reviewed by The Post showed Apple providing detailed location data, as had Google and Facebook.

Others moved to cover their tracks far too late. After days of tweeting death threats to lawmakers and sharing Capitol selfies, saying he had “just wanted to incriminate myself a little lol,” Garret Miller (no known relation to Brandon Miller) had voiced a hint of caution by writing a Facebook post saying that “it might be time for me to ... be hard to locate,” a [criminal complaint](#) states.

That same day, agents obtained a search warrant for his cellphone’s location data, which showed that his phone was inside his Dallas home. When agents arrested him there on Inauguration Day, Miller was wearing a shirt with Trump’s face on it that read, “I Was There, Washington D.C., January 6, 2021,” according to a [filing by prosecutors](#) last month opposing Miller’s release. Miller’s attorneys did not respond to requests for comment.

Another suspected rioter, Damon Beckley, [told](#) Louisville TV station WDRB that he deleted his Facebook account and removed his phone’s SIM card in hopes of evading the FBI. But agents said in a search warrant application that they were still able to match his face in cellphone videos and Capitol photos to his Kentucky driver’s license. (Federal investigators in Kentucky and other states are legally authorized to view state Department of Motor Vehicles records, no subpoena required.)

Investigators also filed a 33-page search warrant with Facebook demanding virtually everything Beckley had done on the site dating back to Nov. 1: all messages, draft messages, posts, comments, photos, videos, audio recordings, video calls, “pokes,” “likes,” “tags,” searches, location check-ins, privacy settings, session times and durations, calendar items, event postings (past and future), friend requests (approved and rejected), address books, friend lists and relationship status updates, as well as all dates, times, IP addresses, location information and other metadata linked to each item, plus any information he’d shared with the company, including his passwords, security questions, home address, phone number and any linked credit cards or bank accounts.

Beckley’s attorney declined to comment. In a Facebook post cited in the warrant, Beckley defended his presence inside the Capitol by writing that he had been “shoved in by Antifa.”

Outside help with facial recognition

In a Facebook video captioned “Peacefully storming the Capital,” a man could be seen shouting, “In the Capitol baby, yeah!” as he joined a mob pushing past broken glass and into the building’s threshold, according to a criminal complaint. The FBI’s Operational Technology Division in Quantico, Va., ran that image through the bureau’s facial recognition search tool, which matched it to the California driver’s license photo of Mark Simon, whom agents called a “known activist” from Huntington Beach. He was arrested in California in January. His attorney did not respond to requests for comment.

Investigators went beyond official databases as well, the documents say. An amateur “sedition hunter” tweeted that the same man seemed to appear in two videos blasting a chemical spray at officers outside the Capitol and later talking about the clash while wearing camouflage pants and a “Guns Save Lives” sticker inside the lobby of an Arlington hotel, according to a criminal complaint.

Agents said they pulled the hotel’s booking reservations, then compared driver’s license photos to the alleged rioter on the video, whom they identified as a Texas man named Daniel Ray Caldwell. In a detention hearing after Caldwell’s arrest, the FBI agent testified that he also “used facial recognition technology to determine whether a picture of Defendant’s face matched with any video on the Internet,” and that the unidentified “software independently found a match” between Caldwell’s photo and the hotel video, according to a magistrate judge’s order last month.

The FBI declined to comment on its facial recognition techniques. Caldwell’s attorney did not respond to requests for comment.

Some cases hinged on facial recognition tips submitted to the FBI by outside agencies. After the FBI published “be on the lookout” bulletins with suspects’ photos, officials at the Harford County state’s attorney’s office in Maryland ran one of the images, of a man inside the Capitol with his mask sunk beneath his chin, through an unnamed piece of facial recognition software, according to a criminal complaint. The tool returned the face of Robert Reeder, smiling for a Maryland driver’s license photo in a gray hoodie like the one the suspect had worn on Jan. 6.

An FBI agent said in the complaint that Reeder cooperated several days later by handing over a mix of photos and videos from his phone showing himself and others surging through the Capitol. Reeder’s attorney declined to comment.

Increasingly pervasive use of facial recognition by local police forces also helped fuel the FBI's nationwide manhunt. After the FBI began asking for help by circulating bulletins with suspects' images, 12 detectives and crime analysts with the Miami Police Department began running the photos through Clearview AI, a facial recognition tool built on billions of social media and public images from around the Web.

Officers signed a contract with the tool's creators last year, hoping for a potential breakthrough: Their other facial recognition search only looks through official photos, such as jail mug shots. But Clearview has faced lawsuits from advocacy groups arguing its technology violates privacy rights, and Google and Facebook have demanded the company stop copying their photos into its searchable database.

The Miami police team has run 129 facial recognition searches through Clearview and sent 13 possible matches to FBI agents for further investigation, said Armando R. Aguilar, assistant chief of the department's Criminal Investigations Division, adding, "We were happy to help however we could."

Clearview AI's chief executive, Hoan Ton-That, declined to provide specifics but said in a statement to The Post that "it is gratifying that Clearview AI has been used to identify the Capitol rioters who attacked our great symbol of democracy."

A passport application and a bank video

Unlike many of the Capitol insurrectionists, Philip Grillo had not immediately given himself away: He wore a mask, did not live-stream himself committing crimes, and stormed the Capitol shouting, "Fight for Trump" while holding a cellphone registered in his mother's name.

But that did not stop the FBI, as agents alleged in a criminal complaint: After two tipsters called the bureau, saying they recognized Grillo on TV, agents trawling through Capitol surveillance camera footage spotted him leaping through a broken window and taking a selfie inside the Rotunda, his mask around his neck.

They compared his face on the video to a photo from Grillo's application for a passport in 2017, the complaint shows, and they matched his embroidered Knights of Columbus jacket with one spotted in a YouTube clip of a violent brawl.

The agents said in the complaint that they also used a Verizon search warrant to determine that Grillo's phone had been inside the Capitol, and they scanned license plate reader data from D.C. to New York, where he had been a Republican Party official in Queens: His Chevrolet Traverse had been spotted leaving New York City the night before and recorded near the Capitol at 2 a.m. the morning of the riot.

Later, photographers spotted Grillo leaving a federal court building in Brooklyn, using a hoodie to cover his face. His attorney declined to comment.

The FBI also has been aided by the online army of self-proclaimed "sedition hunters," like the one who helped identify Caldwell. They scoured the Web for clues to track down rioters and often tweeted their findings publicly in what amounted to a crowdsourced investigation of the Capitol attack. The citizen sleuths organized their pursuits with hashtags: One man, Clayton Mullins, a Kentucky car dealer whose alleged assault of a police officer was captured on YouTube video, was given the viral hashtag "#slickback" for the way he wore his hair.

From that video, a tipster pointed the FBI to Mullins's Kentucky driver's license photo, which allowed FBI investigators to figure out where he had a bank account, according to a criminal complaint. In February, an agent talked to a bank employee, who not only told them Mullins had been there a day before but queued up surveillance video of him talking to a teller, wearing no mask and with his dark hair pushed back in that signature slick.

Mullins, whose attorney declined to comment, was released from federal custody last month on the condition that he not leave his home in western Kentucky, court filings show. His detention will be enforced by a location-tracking GPS monitor.

Spencer S. Hsu, Matt Kiefer and Julie Tate contributed to this report.

Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use

By [Drew Harwell](#)

December 19, 2019 at 6:43 p.m. EST

Facial-recognition systems misidentified people of color more often than white people, a landmark federal study released Thursday shows, casting new doubts on a rapidly expanding investigative technique widely used by law enforcement across the United States.

Asian and African American people were up to 100 times more likely to be misidentified than white men, depending on the particular algorithm and type of search. Native Americans had the highest false-positive rate of all ethnicities, according to the study, which found that systems varied widely in their accuracy.

The faces of African American women were falsely identified more often in the kinds of searches used by police investigators where an image is compared to thousands or millions of others in hopes of identifying a suspect.

Algorithms developed in the United States also showed high error rates for “one-to-one” searches of Asians, African Americans, Native Americans and Pacific Islanders. Such searches are critical to functions including cellphone sign-ons and airport boarding schemes, and errors could make it easier for impostors to gain access to those systems.

Women were more likely to be falsely identified than men, and the elderly and children were more likely to be misidentified than those in other age groups, the study found. Middle-aged white men generally benefited from the highest accuracy rates.

The National Institute of Standards and Technology, the federal laboratory known as NIST that develops standards for new technology, found “empirical evidence” that most of the facial-recognition algorithms exhibit “demographic differentials” that can worsen their accuracy based on a person’s age, gender or race.

The study could fundamentally shake one of American law enforcement’s fastest-growing tools for identifying criminal suspects and witnesses, which privacy advocates have argued is ushering in a dangerous new wave of government surveillance tools.

The FBI alone has logged more than 390,000 facial-recognition searches of state driver's license records and other federal and local databases since 2011, federal records show. Members of Congress this year have voiced anger over the technology's lack of regulation and its potential for discrimination and abuse.

Lawmakers on Thursday said they were alarmed by the "shocking results" and called on the Trump administration to reassess its plans to expand facial recognition use inside the country and along its borders. Rep. Bennie G. Thompson (D-Miss.), chairman of the Committee on Homeland Security, said the report shows "facial recognition systems are even more unreliable and racially biased than we feared."

Sen. Ron Wyden (D-Ore.) said the findings showed how "algorithms often carry all the biases and failures of human employees, but with even less judgment." In a statement, he added, "Any company or government that deploys new technology has a responsibility to scrutinize their product for bias and discrimination at least as thoroughly as they'd look for bugs in the software."

San Francisco, Oakland and two cities in Massachusetts, Somerville and Brookline, have passed bans this year on facial-recognition use by public officials. The state of California also banned the software's use in police body cameras.

The federal report confirms previous studies from researchers who found similarly staggering error rates. Companies such as Amazon had criticized those studies, saying they reviewed outdated algorithms or used the systems improperly.

One of those researchers, Joy Buolamwini, said the study was a "comprehensive rebuttal" to skeptics of what researchers call "algorithmic bias."

"Differential performance with a factor of up to 100?!?" she wrote The Washington Post in an email Thursday. The study, she added, is "a sobering reminder that facial recognition technology has consequential technical limitations alongside posing threats to civil rights and liberties."

Investigators said they did not know what caused the gap but hoped the findings would, as NIST computer scientist Patrick Grother said in a statement, prove "valuable to policymakers, developers and end users in thinking about the limitations and appropriate use of these algorithms."

Jay Stanley, a senior policy analyst at the American Civil Liberties Union, which sued federal agencies earlier this year for records related to how they use the technology, said the research showed why government leaders should immediately halt its use.

"One false match can lead to missed flights, lengthy interrogations, tense police encounters, false arrests, or worse," he said. "But the technology's flaws are only one concern. Face recognition technology — accurate or not — can enable undetectable, persistent, and suspicionless surveillance on an unprecedented scale."

NIST's test examined most of the industry's leading systems, including 189 algorithms voluntarily submitted by 99 companies, academic institutions and other developers. The algorithms form the central building blocks for most of the facial-recognition systems around the world.

The algorithms came from a range of major tech companies and surveillance contractors, including Idemia, Intel, Microsoft, Panasonic, SenseTime and Vigilant Solutions. Notably absent from the list was Amazon, which develops its own software, Rekognition, for sale to local police and federal investigators to help track down suspects.

NIST said Amazon did not submit its algorithm for testing. The company did not immediately offer comment but has said previously that its cloud-based service cannot be easily examined by NIST's test. Amazon founder and chief executive Jeff Bezos owns The Washington Post.

Grother, the NIST lead researcher, said other companies with cloud-based systems had been able to submit their algorithms, including Microsoft, who he said "sent us very capable and very reliable software." Of Amazon, he added: "Our test remains open if they elect to participate."

The NIST team tested the systems with about 18 million photos of more than 8 million people, all of which came from databases run by the State Department, the Department of Homeland Security and the FBI. No photos were taken from social media, video surveillance or the open Internet, they said.

The test studied both how algorithms work on "one-to-one" matching, used for unlocking a phone or verifying a passport, and "one-to-many" matching, used by police to scan for a suspect's face across a vast set of driver's license photos. Investigators tested both false negatives, in which the system fails to realize two identical faces are the same, as well as false positives, in which the system identifies two different faces as being the same — a dangerous failure for police, who could end up arresting an innocent person.

Some algorithms produced few errors, but the disparity in accuracy between different systems could be enormous. There is no national regulation or standard for facial-recognition algorithms, and local law-enforcement agencies rely on a wide range of contractors and systems with different capabilities and levels of accuracy. The algorithms themselves — with names such as "anyvision-004" and "didiglobalface-001" — are almost entirely unknown to anyone outside the industry.

Algorithms developed in Asian countries had smaller differences in error rates between white and Asian faces, suggesting a relationship "between an algorithm's performance and the data used to train it," the researchers said.

"You need to know your algorithm, know your data and know your use case," said Craig Watson, a manager at NIST. "Because that matters."

Ms. JACKSON LEE. I thank, again, our distinguished Witnesses for their attendance and participation. We thank all those who helped prepare this hearing.

Without objection, all Members will have five legislative days to submit additional written questions for the Witnesses or additional materials for the record.

Again, this hearing is adjourned.

Thank you.

[Whereupon, at 1:29 p.m., the Subcommittee was adjourned.]

APPENDIX



July 16, 2021

The Honorable Jerry Nadler
Chair
U.S. House Committee on the Judiciary
2138 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jim Jordan
Ranking Member
U.S. House Committee on the Judiciary
2138 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Sheila Jackson Lee
Chair
U.S. House Crime, Terrorism, and Homeland
Security Subcommittee
2138 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Andy Biggs
Ranking Member
U.S. House Crime, Terrorism, and Homeland
Security Subcommittee
2138 Rayburn House Office Building
Washington, D.C. 20515

Re: Facial Recognition Technology: Examining Its Use by Law Enforcement

On behalf of Color Of Change, we submit this letter for the record in connection with the House Crime, Terrorism, and Homeland Security Subcommittee's hearing "Facial Recognition Technology: Examining Its Use by Law Enforcement," which was held on July 13, 2021.

No amount of regulation or efforts to erase accuracy deficits will make facial recognition a safe tool for law enforcement use. The exchange of Black communities' privacy and due process is not worth the enhanced surveillance of facial recognition technology. Over the past several years, law enforcement use of facial recognition technology has made it clear they cannot be trusted with this dangerous technology because it facilitates racially biased policing. To keep our communities safe, we cannot give law enforcement more invasive surveillance tools. Giving law enforcement facial recognition in hopes of quelling bias is like using gasoline to put out fires. We need to shift the paradigm. Law enforcement will continue disregarding accountability measures, which will obstruct efforts to both track their use of facial recognition technology and regulate abuse of the technology. The threat of facial recognition surveillance could discourage



COLOR OF CHANGE
COLOROFCHANGE.ORG

activity protected by the Constitution and other laws, such as protesting or obtaining a driver's license, creating a surveillance network that will impact us all.¹

Law enforcement use of facial recognition technology is accelerating biased policing. Law enforcement entities have demonstrated they will use this technology to violate our constitutional rights. Facial recognition technology threatens to completely erase our privacy and expose Black people to more surveillance and overpolicing. For these reasons, Color Of Change believes law enforcement should not have access to this technology. **We encourage Congress to pass a federal ban on law enforcement use of facial recognition and other biometric surveillance technology.**

Law enforcement use of facial recognition technology perpetuates racial bias. Facial recognition technology gives law enforcement a tool that enhances the discriminatory surveillance and policing of Black communities.² The technology gives police an “objective” reason to continue targeting the Black and brown communities they have always surveilled.³ When police departments use facial recognition technology in connection with mugshot databases to find suspects, they rely on a pool reflecting the racial bias of the criminal justice system.⁴ In this reinforcement loop, Black people are disproportionately arrested and therefore overrepresented in these databases. The use of facial recognition technology to find investigative leads will direct law enforcement to return to people who have histories with police, thus further implicating them for past behavior. Facial recognition technology can create a vicious cycle, keeping people in constant contact with law enforcement.

Law enforcement agencies ignore policies put in place to prevent abuse of facial recognition technology. There is a long history of law enforcement misusing surveillance technology to

¹ Clare Garvie, “Public Protest, Face Recognition, and the Shield of Anonymity,” Medium, June 9, 2020, <https://medium.com/center-on-privacy-technology/public-protest-face-recognition-and-the-shield-of-anonymity-44d8a8ad1e80>; Drew Harwell and Erin Cox, “ICE has run facial-recognition searches on millions of Maryland drivers,” *The Washington Post*, February 26, 2020, <https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers/>.

² Tawana Petty, “Defending Black Lives Means Banning Facial Recognition,” *Wired*, July 10, 2020, <https://www.wired.com/story/defending-black-lives-means-banning-facial-recognition/>.

³ Annie Gilbertson, “Data-Informed Predictive Policing Was Heralded As Less Biased. Is It?” *The Markup*, August 20, 2020, <https://themarkup.org/ask-the-markup/2020/08/20/does-predictive-police-technology-contribute-to-bias>; Rashida Richardson, Jason Schultz, and Kate Crawford, “Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice,” 94 N.Y.U. L. Rev. Online 192, 218-19 (2019) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333423.

⁴ Claire Garvie, Alvaro Bedoya, and Johnathan Frankle, “The Perpetual Line-Up,” Center on Privacy & Technology at Georgetown Law, October 18, 2016, <https://www.perpetuallineup.org/findings/racial-bias>; John Kelly, “Analysis of police arrests reveals stark racial disparity in NY, NJ and CT,” ABC 7 New York, June 10, 2020, <https://abc7ny.com/police-racial-bias-profiling-disparity-in-arrests-black-arrest-rates/6241175/>.



target Black activists, and facial recognition technology is no different. Law enforcement misuse of facial recognition will disproportionately harm Black activists. We cannot trust that new regulations will be enough to protect our communities. During last summer's uprisings, New York City police went to the home of Derrick Ingram, a Black Lives Matter activist, to arrest him. Police submitted a photo to their facial recognition technology to locate him using what appeared to be a photo taken from his Instagram account.⁵ In doing so, New York City police violated their own policy, which states that facial recognition technology can only be used with a still from a surveillance video or an arrest photo.⁶ This behavior is typical of what we should expect; any limitations on policy are unlikely to be followed by police. We will continue to see law enforcement use facial recognition to target and harass leaders and organizers in the Black community unless Congress prohibits their use of the technology.

Law enforcement officers have also demonstrated they will routinely misuse facial recognition software. A report from the Center on Privacy & Technology at Georgetown Law detailed the New York Police Department's (NYPD) frequent tampering of photos submitted to their facial recognition technology.⁷ Making changes to a photograph to find an investigative lead could dramatically alter the results a search will yield. Facial recognition systems work best with well-lit photographs where the subject is looking at the camera. The report found that when police do not have quality photos, they turn to other options. The NYPD used a photo of Woody Harrelson to find a suspect who they thought looked like him on the surveillance footage.⁸ The department also used a photo of a New York Knicks player to find another suspect.⁹

Police have also used artist sketches in lieu of photographs, despite research showing that facial recognition systems work best with photographs.¹⁰ In other instances, police edited a suspect photo, adding a different mouth, before submitting it to the facial recognition software.¹¹ The choice between one mouth shape versus another or one eye shape versus another can mean the difference between an innocent person being left undisturbed or being arrested. When it comes to

⁵ George Joseph and Jake Offenhartz "NYPD Used Facial Recognition Technology in Siege of Black Lives Matter Activist's Apartment," Gothamist, August 14, 2020,

<https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment>.

⁶ James Vincent, "NYPD used facial recognition to track down Black Lives Matter activist," The Verge, August 18, 2020,

<https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram>.

⁷ Clare Garvie, "Garbage In, Garbage Out: Face Recognition on Flawed Data," Center on Privacy & Technology at Georgetown Law, <https://www.flawedfacedata.com/>.

⁸ *Ibid.*

⁹ *Ibid.*

¹⁰ Anil K. Jain, Brendan Klare, and Unsang Park, "Face Recognition: Some Challenges in Forensics," 2011 *IEEE International Conference on Automatic Face & Gesture Recognition (FG)*, 2011, pp. 726-733, <https://ieeexplore.ieee.org/document/5771338>.

¹¹ Clare Garvie, "Garbage In, Garbage Out," Center on Privacy & Technology at Georgetown Law, May 16, 2019, <https://www.flawedfacedata.com/>.



Black communities, the difference between being undisturbed and being arrested can mean the difference between life and death. This pattern of misuse, often permitted or encouraged by department protocols, suggests that law enforcement use of facial recognition technology cannot be reformed.¹² If law enforcement continue to have access to this technology, they will continue to misuse it and put Black communities at risk.

Discriminatory use of facial recognition technology is exacerbated by the algorithms' documented racial bias.¹³ Robert Williams and Nijeer Parks were both falsely arrested after police improperly relied on facial recognition searches.¹⁴ In Mr. Williams' case, police arrested him although he did not look like the picture of the suspect captured at the crime scene.¹⁵ These are two stories where we know law enforcement used facial recognition to arrest the wrong person. But there are other untold stories of innocent Black people who have been targeted because of this technology. **Mediocre law enforcement use, racist motivation, and flawed algorithms make facial surveillance too dangerous a tool for law enforcement to have at the expense of the freedom and safety of Black communities.**

Law enforcement use of facial recognition technology raises significant accountability concerns. Law enforcement offer no transparency in their use of facial recognition technology. This makes it difficult to hold them accountable and for defendants to get true due process. This June, the Government Accountability Office published a report on the use of facial recognition technology by federal agencies.¹⁶ However, five agencies did not report their use of Clearview AI between April 2018 and March 2020, even though public records indicate that those agencies indeed used the technology.¹⁷ If law enforcement do not honestly disclose their use of these systems, it will naturally make efforts to regulate them more complicated. As has been proven,

¹² *Ibid.*

¹³ Joy Buolamwini and Timnit Gebru, "Gender Shades," MIT Media Lab, 2018, <http://gendershades.org/overview.html>; Sophie Bushwick, "How NIST Tested Facial Recognition Algorithms for Racial Bias," Scientific American, December 27, 2019, <https://www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias/>.

¹⁴ Kashmir Hill, "Wrongfully Accused by an Algorithm," *The New York Times*, June 24, 2020, <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>; David K. Li, "Black man in New Jersey misidentified by facial recognition tech and falsely jailed, lawsuit claims," NBC News, December 29, 2020, <https://www.nbcnews.com/news/us-news/black-man-new-jersey-misidentified-facial-recognition-tech-falsely-jailed-n1252489>.

¹⁵ Hill, "Wrongfully Accused by an Algorithm," *The New York Times*, June 24, 2020, <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>.

¹⁶ "Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks," Government Accountability Office, June 29, 2021, <https://www.gao.gov/products/gao-21-518>.

¹⁷ Caroline Haskins and Ryan Mac, "A Government Watchdog May Have Missed Clearview AI Use by Five Federal Agencies in a New Report," BuzzFeed News, June 30, 2021, <https://www.buzzfeednews.com/article/carolinehaskins1/gao-facial-recognition-report-clearview-federal-agencies>.



Congress and federal watchdogs cannot rely on law enforcement to self-regulate their use of facial recognition technology.

When law enforcement do not inform defendants that facial recognition technology was used to target them as suspects, their defense attorneys lose an opportunity to challenge the procedure. Facial recognition technology should not be used at all; however, if it is deployed, it should be used for investigative leads rather than a conclusive end. If law enforcement use it to either further their investigation or make conclusions, defense attorneys should be made aware to best prepare their clients' case.¹⁸ In the case of Willie Lynch, Jacksonville Sheriff's Office detectives used facial recognition to find a suspect. The system returned a line-up that included Mr. Lynch and gave him a one-star rating, indicating that he was a poor match to the photo submitted.¹⁹ His defense attorneys could have used the low-confidence score—or information regarding whether or not the police further investigated the other leads before arresting him—to bolster Mr. Lynch's case. But when law enforcement withhold this information from discovery, defense attorneys cannot give zealous representation for their clients, which severely disadvantages defendants.

The use of facial recognition may discourage people from protesting injustice.²⁰ The Baltimore Police Department used facial recognition technology during the 2015 uprising following the murder of Freddie Gray.²¹ Other police departments have also requested photographs of protesters during the 2020 uprisings, presumably for facial recognition technology.²² As noted, this tech was used to arrest Mr. Ingram in New York City. Our communities have historically used the right to publicly assemble and protest to secure justice. Facial recognition technology will disrupt this right.

Law enforcement do not currently offer communities ways to meaningfully opt out of the use of facial recognition technology. In Maryland, immigrants are authorized to get driver's licenses. When they signed up for the privilege, they were not pre-warned that Immigration and Customs Enforcement (ICE) would have access to the photo database.²³ ICE was permitted to run facial

¹⁸ Aaron Mak, "Facing Facts," Slate, January 25, 2019, <https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html>.

¹⁹ *Ibid.*

²⁰ Clare Garvie, "Public Protest, Face Recognition, and the Shield of Anonymity," Medium, June 9, 2020, <https://medium.com/center-on-privacy-technology/public-protest-face-recognition-and-the-shield-of-anonymity-44d8a8ad1e80>.

²¹ "Baltimore County Police Department and Geofeedia Partner to Protect the Public During Freddie Gray Riots," The ACLU of Northern California, 2016, https://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf.

²² Caroline Haskins, "Dallas Police Asked People to Call Out Protesters. People Flooded Their App with K-Pop Instead," BuzzFeed News, June 1, 2020, <https://www.buzzfeednews.com/article/carolinehaskins1/dallas-police-kpop>.

²³ Drew Harwell and Erin Cox, "ICE has run facial-recognition searches on millions of Maryland drivers," *The Washington Post*, February 26, 2020,



recognition searches without seeking state or court approval. **The use of facial recognition technology to conduct immigration enforcement will have counterproductive effects, discouraging people from participating in an effort to maintain public safety**

Facial recognition technology training and development rely on surveillance and violations of privacy. Clearview AI allows users to find individuals based on the photos they upload to their social media platforms.²⁴ This service builds on and furthers the surveillance economies created by the Tech Giants, thus contributing data points to an already biased algorithm. Despite Clearview AI violating the terms of service of the platforms they scraped, Google, Facebook, Twitter, and others were powerless to hold the company accountable for its actions. Clearview AI is not the only system that uses our data for their facial recognition system. The Federal Trade Commission concluded that Everalbum, a photo-sharing platform, created its facial recognition system using deceptive practices.²⁵ Everalbum trained its algorithms on user photos. However, users of the platform neither consented nor would reasonably expect their pictures to be used in this way. The Commission found that this deceptive practice would allow Everalbum to profit from wrongdoing and ordered the company to destroy the facial recognition algorithm. Google contractors used deception to get photos of darker-skinned people to improve the Pixel 4's facial recognition system.²⁶ These contractors targeted Black people experiencing homelessness and offered \$5 gift cards without disclosing what the pictures would be used for.

Color Of Change urges the Crime, Terrorism, and Homeland Security Subcommittee to consider the disproportionate impact facial recognition technology will have on Black communities. We endorsed Representatives Jayapal, Pressley, and Tlaib's Facial Recognition and Biometric Technology Moratorium Act, which would ban the use of facial recognition technology and other biometric surveillance technology by federal entities.²⁷ **Banning facial recognition technology is an urgent racial justice issue.** Our communities need robust protection from surveillance and overpolicing. This technology cannot be reformed and must be removed from the law enforcement toolkit.

<https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers/>.

²⁴ Kashmir Hill, "The Secretive Company That Might End Privacy As We Know It," *The New York Times*, January 18, 2020, <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

²⁵ "In the Matter of Everalbum, Inc.," Federal Trade Commission, May 7, 2021,

https://www.ftc.gov/system/files/documents/cases/everalbum_complaint.pdf.

²⁶ Jennifer Elias, "Google contractor reportedly tricked homeless people into face scans," CNBC, October 3, 2019, <https://www.cnn.com/2019/10/03/google-contractor-reportedly-tricked-homeless-people-into-face-scans.html>.

²⁷ "Press Release: Jayapal and Lawmakers Introduce Bicameral Legislation to Ban the Use of Facial Recognition Technology by the Government," <https://jayapal.house.gov/2021/06/15/ban-facial-recognition-tech/>; "Facial Recognition and Biometric Technology Moratorium Act of 2021,"

https://www.markey.senate.gov/imo/media/doc/facial_recognition_and_biometric_technology_moratorium_act.pdf.



COLOR OF CHANGE
COLOROFCHANGE.ORG

If you have questions, please contact Color Of Change's president, Rashad Robinson (rashad@colorofchange.org).

Sincerely,



Rashad Robinson
President
Color Of Change



New York Office
40 Rector Street, 5th Floor
New York, NY 10006-1738

T 212.905.2200
F 212.229.7892

www.naacpldf.org



Washington, D.C. Office
700 14th Street, NW, Suite 600
Washington, D.C. 20005

T 202.682.1900
F 202.682.1512

July 20, 2021

Submitted via electronic mail (Arya.Hariharan@mail.house.gov)

Chairwoman Sheila Jackson Lee
House of Representatives
2426 Rayburn House Office Building
Washington, DC 20515

Ranking Member Andy Biggs
House of Representatives
171 Cannon House Office Building
Washington, DC 20515

**RE: July 13, 2021 Subcommittee on Crime, Terrorism, and Homeland Security
Hearing on Law Enforcement Use of Facial Recognition Technology**

Dear Chairwoman Jackson Lee and Ranking Member Biggs:

On behalf of the NAACP Legal Defense and Educational Fund, Inc. (LDF), we submit this letter for the record in connection with the July 13, 2021 hearing held by the House Judiciary Committee's Subcommittee on Crime, Terrorism, and Homeland Security titled "Facial Recognition Technology: Examining Its Use by Law Enforcement."

LDF is the nation's first and foremost civil rights legal organization devoted to racial justice. Since its founding in 1940, LDF has worked at the national, state, and local levels to achieve racial justice and eliminate structural barriers for African-Americans in the areas of criminal justice, economic justice, education, and political participation.¹ As part of that work, LDF has forged longstanding partnerships with advocates, activists, and attorneys to challenge and reform unlawful and discriminatory policing practices across the country, including law enforcement's use of technology and automation in a racially discriminatory manner.²

¹ *About Us*, NAACP LDF, <https://www.naacpldf.org/about-us/>; see also, *Shepherd v. Florida*, 341 U.S. 50 (1951) (reversing the convictions of Black men falsely accused of raping a white woman in 1949 after sheriff's deputies brutally beat the men to force them to falsely confess).

² See e.g., *LDF Sends Letter Expressing Concerns Over NYPD's Compliance with the P.O.S.T. Act*, NAACP LDF (February 24, 2021), <https://www.naacpldf.org/news/ldf-sends-letter-expressing-concerns-over-nypds-compliance->





With this extensive experience, we submit this letter to highlight the disproportionate threat that facial recognition technology imposes on communities of color when used by law enforcement. Due to the concerns highlighted below, law enforcement agencies should not be authorized to use facial recognition technology.

1. Both Historically and in Present-Day, Law Enforcement Practices Have Disproportionately Criminalized Black and Brown Communities

There is a history of police surveilling and racially targeting Black people and communities of color in the United States. Today, law enforcement practices continue to produce racial disparities and police violence towards communities of color.

The first police forces in the United States were infamously formed to patrol enslaved people and preserve the system of slavery.³ Throughout our history, American law enforcement forces have used state power to track, monitor and control the lives and movements of Black people.⁴ Specifically, police have enforced segregation and Jim Crow laws, supported the disenfranchisement of Black Americans, and used their power and tools to inflict brutal force, unlawfully arrest, and criminalize Black and Brown communities.⁵ These decades-long patterns

[with-the-post-act/](#); *Testimony of Janai Nelson before the NYC Automated Decision Systems Task Force* (April 30, 2019), <https://www1.nyc.gov/assets/adstaskforce/downloads/pdf/ADS-Public-Forum-Comments-NAACP-LDF.pdf>; *Public Comment on the NYPD's Draft Impact & Use Policies for the Criminal Group Database and Social Network Analysis Tools* (February 25, 2021), <https://ccrjustice.org/sites/default/files/attach/2021/02/Written%20Comment%20on%20NYPD%27s%20Draft%20a%20Use%20Policies%20for%20the%20Gang%20Database%20and%20Social%20Network%20Analysis%20Too%20Is%20BxD%20CCR%20LAS%20LDF.pdf> (joining Bronx Defenders, Center for Constitutional Rights, and the Legal Aid Society to address the impact and use of the NYPD's Criminal Group Database and Social Network Analysis Tools).

³ Olivia B. Waxman, *How the U.S. Got Its Police Force*, TIME (May 18, 2017), <https://time.com/4779112/police-history-origins/> ("In the South, however, the economics that drove the creation of police forces were centered not on the protection of shipping interests but on the preservation of the slavery system."); *The History Of Policing And Race In The U.S. Are Deeply Intertwined*, NPR (June 13, 2020), <https://www.npr.org/2020/06/13/876628302/the-history-of-policing-and-race-in-the-u-s-are-deeply-intertwined>.

⁴ See Connie Hassett-Walker, *How You Start is How You Finish? The Slave Patrol and Jim Crow Origins of Policing*, AMERICAN BAR ASSOCIATION (January 12, 2021), https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/civil-rights-reimagining-policing/how-you-start-is-how-you-finish/; Jill Lepore, *The Invention of Police*, THE NEW YORKER (July 13, 2020), <https://www.newyorker.com/magazine/2020/07/20/the-invention-of-the-police> ("Progressive-era policing criminalized blackness . . . police patrolled Black neighborhoods and arrested Black people disproportionately; prosecutors indicted Black people disproportionately; juries found Black people guilty disproportionately; judges gave Black people disproportionately long sentences.").

⁵ See Waxman, *supra* note 3; see generally, ELIZABETH K. HINTON, AMERICA ON FIRE: THE UNTOLD HISTORY OF POLICE VIOLENCE AND BLACK REBELLION SINCE THE 1960s (2021).



of discrimination and violence at the hands of law enforcement sparked widespread protests against police brutality in the early 1960s, throughout the 20th century, and they continue today.⁶

Racially discriminatory police practices are still prevalent.⁷ While former Minneapolis police officer Derek Chauvin's callous murder of George Floyd and the subsequent widespread public outcry drew the nation's attention to deep-seated racism in policing, many other victims of discriminatory police violence remain unknown. Numerous U.S. Department of Justice (DOJ) investigations, state and federal courts findings, and reports have documented patterns of unconstitutional, unlawful, and/or racially discriminatory policing practices.⁸ Police killings are the sixth leading cause of death in Black men,⁹ and people of color make up 46% of all arrests and 57% of all those incarcerated nationwide.¹⁰

Facial recognition technology risks exacerbating these racially discriminatory policing practices by expanding the reach of law enforcement into Black and Brown communities using unreliable and faulty technology. If law enforcement is permitted to continue using these technologies, it will perpetuate and likely increase the systemic racism reflected in historic and current policing practices.

⁶ The Watts Riots of the 1960s are a glaring example of uprisings that spawned from police violence. See Morgan Jerkins, *She Played a Key Role in the Police Response to the Watts Riots. The Memory Still Haunts Her—But Black History is Full of Haunting Memories*, TIME (August 3, 2020), <https://time.com/5873228/watts-riots-memory/>.

⁷ Radley Balko, *There's overwhelming evidence that the criminal justice system is racist. Here's the proof.*, WASHINGTON POST (June 10, 2020), <https://www.washingtonpost.com/graphics/2020/opinions/systemic-racism-police-evidence-criminal-justice-system/#DrugWar>.

⁸ See e.g., *Davis v. City of N.Y.*, 10 Civ. 0699 (SAS) (S.D.N.Y. May 5, 2011); *Floyd v. City of N.Y.*, 959 F. Supp. 2d 540 (S.D.N.Y. 2013); Civil Rights Division, U.S. Department of Justice, *Investigation of the Ferguson Police Department* (March 4, 2018), https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/ferguson_police_department_report.pdf; Civil Rights Division, U.S. Department of Justice, *Investigation of the Baltimore City Police Department* (Aug. 10, 2016), <https://www.justice.gov/crt/file/883296/download>; Civil Rights Division, U.S. Department of Justice, *Investigation of the New Orleans Police Department* (March 16, 2011), https://www.justice.gov/sites/default/files/crt/legacy/2011/03/17/nopd_report.pdf; Civil Rights Division, U.S. Department of Justice, *LAPD Notice of Investigation Letter* (May 8, 2000), <https://www.justice.gov/crt/lapd-notice-investigation-letter>.

⁹ See Frank Edwards et. al., *Police: Sixth-leading cause of death for young Black men*, University of Michigan (Aug. 5, 2019), <https://news.umich.edu/police-sixth-leading-cause-of-death-for-young-black-men/>.

¹⁰ 2019 *Crime in the U.S. Report: Arrests by Race and Ethnicity*, U.S. Department of Justice (2019), <https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/tables/table-43>.



2. Law Enforcement Use of Facial Recognition Technology Risks Disproportionally Exposing Black and Brown People to Misidentification and Perpetuates Heightened Surveillance of Their Communities

Communities of color are over-policed,¹¹ and law enforcement officers have far too much discretion¹² with insufficient oversight.¹³ Permitting law enforcement officers and agencies to use facial recognition technology risks exacerbating already existing racial inequities and the disparate criminalization of Black and Brown people.¹⁴ Already, police have used other forms of technology and automation to disproportionately target Black and Brown communities, reiterating historical

¹¹ See sources cited *supra* note 8; Drew Desilver et al., *10 things we know about race and policing in the U.S.*, PEW RESEARCH CENTER (June 3, 2020) <https://www.pewresearch.org/fact-tank/2020/06/03/10-things-we-know-about-race-and-policing-in-the-u-s/> (“Black adults are about five times as likely as whites to say they’ve been unfairly stopped by police because of their race or ethnicity.”).

¹² See e.g., DOJ investigative report into the Ferguson Police Department (March 4, 2015), https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/ferguson_police_department_report.pdf (noting the influx of police arrests of Black residents for charges within the officer’s discretion; “Ferguson police ‘persistently exercise[d] discretion to the detriment of African Americans’”); see also Jeffrey S. Nowacki, *Police discretion, organizational characteristics, and traffic stops: An analysis of racial disparity in Illinois*, 21 INTERNATIONAL JOURNAL OF POLICE SCIENCE AND MANAGEMENT 1, 4-16 (2019), <https://journals.sagepub.com/doi/pdf/10.1177/1461355719832617> (noting similar trends of increased police traffic stops and subsequent charges on African American motorists, when the stop or charge relied upon police discretion, prompting the phrase “driving while Black”).

¹³ See Degroff & Cahn, *An Early Assessment of Community Control of Police Surveillance Laws*, SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT (February 10, 2021), <https://static1.squarespace.com/static/5c1bfc7ee175995a4ceb638/t/602430a5ef89df2ce6894ce1/1612984%20485653/New+CCOPS+On+The+Beat.pdf> (noting that while some local and state ordinances have begun to require oversight on police use of technology, compliance is limited, and noting the lack of a governing and uniform oversight guidance); see also, Petition at 3, *Amnesty International v. N.Y.C. Police Department* (N.Y.S. filed July 15, 2021), <https://static1.squarespace.com/static/5c1bfc7ee175995a4ceb638/t/60f0cf1946c0d74f87da1cc7/1626394396185/Venue+Petition.pdf> (suing New York City Police Department over the agency’s refusal to disclose public records about its acquisition of facial recognition technology and other surveillance tools); see also, Leandra Bernstein, *America has 18,000 police agencies, no national standards; experts say that’s a problem*, WJLA (June 9, 2020), <https://wjla.com/news/nation-world/america-has-18000-police-agencies-no-national-standards-experts-say-thats-a-problem>.

¹⁴ See generally Degroff & Cahn, *supra* note 13; see also Radley Balko, *There’s overwhelming evidence that the criminal justice system is racist. Here’s the proof.*, WASHINGTON POST (June 10, 2020), <https://www.washingtonpost.com/graphics/2020/opinions/systemic-racism-police-evidence-criminal-justice-system/#DrugWar>.



trends. For example, predictive policing tools,¹⁵ drones,¹⁶ license plate readers,¹⁷ aerial surveillance,¹⁸ surveillance cameras,¹⁹ and shot spotters,²⁰ have all been used disproportionately against, and resulted in heightened surveillance, over-policing, and/or increased arrest or incarceration, of communities of color.²¹

Furthermore, law enforcement use of facial recognition technology has resulted in the wrongful incarceration of people of color. Facial recognition algorithms frequently are unable to recognize or misidentify individuals with darker skin, features often associated with Black individuals, women, and people who are transgender or nonbinary, resulting in increased error rates in the technology's application to these groups.²² In fact, a report by the National Institute of Standards and Technology found that Black and Asian individuals may be between ten and up to *one hundred* times more likely to be misidentified by facial recognition technology than white

¹⁵ Rachel Levinson-Waldman and Erica Posey, *Court: Public Deserves to Know How NYPD Uses Predictive Policing Software*, THE BRENNAN CENTER (Jan. 26, 2018), <https://www.brennancenter.org/blog/court-rejects-nypd-attempts-shield-predictive-policingdisclosure>; see also Will Douglas Heaven, *Predictive Policing Algorithms are Racist. They Need to be Dismantled*, MIT TECHNOLOGY REVIEW (July 17, 2020), <https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/>.

¹⁶ Faine Greenwood, *How to regulate police use of drones*, BROOKINGS (September 24, 2020), <https://www.brookings.edu/techstream/how-to-regulate-police-use-of-drones/> (describing law enforcement's use of drones to spy on alleged drug deals and homeless encampments, and to arrest three Black Lives Matter protesters).

¹⁷ George Joseph, *What Are License-Plate Readers Good For? Automatic plate-readers catch few terrorists or violent criminals, but do plenty of harm to low-income communities of color*, BLOOMBERG NEWS (August 5, 2016), <https://www.bloomberg.com/news/articles/2016-08-05/license-plate-readers-catch-few-terrorists-but-lots-of-poor-people-of-color>.

¹⁸ Denise Lavoie, *Court finds Baltimore aerial surveillance unconstitutional*, ASSOCIATED PRESS (June 24, 2021), <https://apnews.com/article/baltimore-courts-503b2eb629abf94c25edf4111baf64bd>.

¹⁹ Surveillance city: NYPD can use more than 15,000 cameras to track people using facial recognition in Manhattan, Bronx and Brooklyn, AMNESTY INTERNATIONAL (June 3, 2021), <https://www.amnesty.org/en/latest/news/2021/06/scale-new-york-police-facial-recognition-revealed/> (NYC's cameras are concentrated in neighborhoods with 54% Black and 30% Hispanic populations).

²⁰ Todd Feathers, *Gunshot-Detecting Tech Is Summoning Armed Police to Black Neighborhoods*, VICE (July 19, 2021), <https://www.vice.com/en/article/88nd3z/gunshot-detecting-tech-is-summoning-armed-police-to-black-neighborhoods?fbclid=IwAR3W9CjNaIQVLHk8JmIFG85RKIwHYcBAfuqTRVv5iSziwkh-uyC4sa43gg> (finding that ShotSpotter frequently generates false alerts and deployed almost exclusively in non-white neighborhoods).

²¹ Rashida Richardson, et al., *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 NYU L. REV. 192 (2019), <https://www.nyulawreview.org/wpcontent/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf>.

²² Tom Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally*, WIRED (July 22, 2019), <https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/>; Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, ACLU (July 26, 2018), <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>; Joy Buolamwini, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in 81 PROCEEDINGS OF MACHINE LEARNING RESEARCH 1, 1–15 (2018), <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>.



men, depending on the algorithm used.²³ In the policing context, these misidentifications are particularly dangerous because they can result in false arrests and wrongful incarceration.²⁴

Additionally, despite an algorithm's inaccuracy in identifying people of color, when using facial recognition technologies, law enforcement officers are able to submit *any* photo of an unidentified person to a facial recognition algorithm.²⁵ This may include a poor and low-quality security camera photo, social media photos covered with filters, hand-drawn composite and artist sketches, and even police-edited photos where officers have digitally inserted, removed, or edited facial features.²⁶ This calls into question the credibility of the photos used and compounding the risk of misidentification.

²³ See Patrick Grother et al., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NAT'L INST. STAND. TECHNOL. INTERAG. INTERN. REP. 8280, 2 (December 2019), <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf> (evaluating 189 software algorithms from 99 developers on their ability to correctly identify individuals in 1) one-to-one matching and 2) one-to-many matching, two of the most common uses of facial recognition technology); see also Nat'l Inst. of Standards & Tech., *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software* (Dec. 19, 2019), <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>.

²⁴ See e.g. Complaint at 1, *Williams v. City of Detroit*, No. 2:19-cv-12538 (E.D. Mich. Mar. 24, 2021), ECF No. 1 https://www.aclumich.org/sites/default/files/field_documents/001_complaint_1.pdf (Mr. Williams' lawsuit against the City of Detroit due to wrongful arrest using facial recognition technology); Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, NEW YORK TIMES (updated Jan. 6, 2021), <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>; Elisha Anderson, *Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit*, DETROIT FREE PRESS (July 11, 2020), <https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/>.

²⁵ See Clair Garvey, *Garbage In, Garbage Out: Facial Recognition on Flawed Data*, GEORGETOWN CENTER ON LAW AND PRIVACY (May 16, 2019), <https://www.flawedfacedata.com/> (noting that NYPD and other agencies have used 3D software to "complete," "normalize" and/or rotate partial images of faces that are turned away from the camera to run a search using facial recognition technology).

²⁶ *Id.* (citing examples of policing conducting a Google search for Black features and manually adding them onto the photo and also noting that, because the algorithm cannot distinguish between the parts of the face that were in the original photo and the parts that were either computer generated or added in by a detective, the original photo could represent 60% of a suspect's face, and yet the algorithm could return a possible match assigned a 95% confidence rating, suggesting a high probability of a match to the detective running the search); see also NYPD, *Real Time Crime Center FIS Presentation: Partial Face* (Sept. 17, 2018), Document pp. 025423, 025466 https://drive.google.com/file/d/18vVMSMABlqcE_nAIGf9XRlUUnik8xWOH/view ("The goal was to create an image which highlighted the pronounced facial features of the suspect in this image. [Hairline, Forehead, Brows, and Nose]. The FIS Investigator utilized the head of [redacted] in the previous case mentioned because of the similarities to the hairline and forehead. Both photos were combined within the Photoshop software and a Virtual Probe was created."); Brendan F. Klare et al., *Matching Forensic Sketches to Mug Shot Photos*, 33 IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE 639, 645 (March 2011) (addressing the difficulty of using forensic sketches with facial recognition because "[f]orensic sketches are often an incomplete and poor portrayal of the subject's face.").



There are no defined limits on how or when in their investigative processes law enforcement agencies may use these misidentifications or “possible” matches from facial recognition technology to identify, apprehend, or arrest suspects. And even if an agency specifies in its departmental policy that returned matches from facial recognition technology must be coupled with additional evidence corroborating the assumed identity, there are no federal guidelines on what additional evidence is needed before police can arrest the “identified” person from the search.²⁷ Accordingly, in many instances people of color are being subjected to wrongful criminal arrest and prosecution due to faulty and discriminatory identifications using facial recognition technology.²⁸ While Mr. Robert Williams testified during the hearing about his harrowing wrongful arrest and detention resulting from police use of facial recognition technology, we do not know how many other people have been similarly impacted.²⁹ Coupling the risk and harms of facial recognition technology inaccurately identifying communities of color, with the racial biases and discrimination already reflected in law enforcement and the criminal legal system more broadly, makes law enforcement’s use of this technology particularly dangerous for Black and Brown communities.³⁰

Even if facial recognition technology accurately identified people of all races, ethnicities, and genders, it is still too dangerous to permit its use by law enforcement. Increasingly, law enforcement agencies use tools that facilitate mass surveillance, such as networks of cameras and drones, in predominantly Black and Brown neighborhoods and cities.³¹ Complex networks of

²⁷ Lauren Feiner and Annie Palmer, *Rules Around Facial Recognition and Policing Remain Blurry*, CNBC (June 12, 2021), <https://www.cnbc.com/2021/06/12/a-year-later-tech-companies-calls-to-regulate-facial-recognition-met-with-little-progress.html> (Discussing how Congress has not passed any laws regulating police use of facial recognition technology in the year since Amazon, Microsoft, and IBM committed to halting the sale of facial recognition software to police departments).

²⁸ See sources cited *supra* note 24.

²⁹ See Facial Recognition Technology: Examining its Use By Law Enforcement, Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security, 117 Cong. (July 13, 2021) (Testimony of Robert Williams), <https://docs.house.gov/meetings/JU/JU08/20210713/113906/HMTG-117-JU08-Wstate-WilliamsR-20210713.pdf> (Williams, a Black man, testified that police arrested him at his home and held him in jail for over 30 hours based on an erroneous facial recognition identification).

³⁰ See Degroff & Cahn, *supra* note 13; BRIAN JEFFERSON, *DIGITIZE AND PUNISH: RACIAL CRIMINALIZATION IN THE DIGITAL AGE* (2020), <https://www.jstor.org/stable/10.5749/j.ctvz0h9s7> (highlighting the increased number of Black people registered in police databases and therefore exposed to increased criminalization; “[d]igital databases, not detention centers . . . are becoming the leading edge of criminal justice in the United States. While more than 2 million people are incarcerated . . . the Bureau of Justice Statistics estimates that 100,596,300 names are stored in criminal history databases. In some cities, 80 percent of the black male population is registered in these databases.”); see also Devon W. Carbado, *From Stopping Black People to Killing Black People: The Fourth Amendment Pathways to Police Violence*, 105 CALIF. L. REV. 125, 139 (2017) (“[R]acial profiling exposes African Americans not only to the violence of ongoing police surveillance and contact but also to the violence of serious bodily injury and death.”).

³¹ See AMNESTY INTERNATIONAL, *supra* note 19 (noting that NYC’s cameras are concentrated in neighborhoods with 54% Black and 30% Hispanic populations); see also Noah Urban et al., *A Critical Summary of Detroit’s Project Green*



thousands of cameras span entire neighborhoods, allowing for the police monitoring of an individual's every move the moment they step outside their homes.³² Adding facial recognition to these already-invasive law enforcement tools permits the identification of nearly all persons in the surveilled area and allows police to record individuals' daily routines, associations, locations, and movements—all without having any individualized suspicions of criminal activity in violation of the Constitution.³³ For example, the Fourth Circuit recently considered the use of the Baltimore Police Department's aerial surveillance system that “track[ed] every movement” of every person outside in Baltimore” and was akin to “attaching an ankle monitor” to every person in the city.”³⁴ For the Baltimore residents living in neighborhoods, police now had “an intimate window” into each person’s associations and activities.”³⁵ The Court found that, because the aerial surveillance technology “enable[d] police to deduce from the whole of individuals’ movements,” the agency’s accessing of its data amounted to a warrantless search, violating the Fourth Amendment.³⁶

Law enforcement agencies have also used the heightened surveillance abilities that facial recognition technology provides to target Black activists who speak out about biased policing and police brutality, such as members of Black Lives Matter groups.³⁷ In fact, six federal law enforcement agencies reported using facial recognition technology for criminal investigations related to the 2020 nationwide protests against police brutality.³⁸ In August 2020 for example,

Light and its Greater Context, DETROIT COMMUNITY TECHNOLOGY PROJECT (June 9, 2019), https://detroitcommunitytech.org/system/ldf/librarypdfs/DCTP_PGL_Report.pdf?file=1&type=node&id=77&force= (“There is a legitimate fear regarding what [facial recognition] would look like in a majority black city such as Detroit.”); Timothy Williams, *Can 30,000 Cameras Help Solve Chicago’s Crime Problem?*, NEW YORK TIMES (May 26, 2018), <https://www.nytimes.com/2018/05/26/us/chicago-police-surveillance.html> (“It’s now been normalized for these [low-income] communities to be under constant surveillance, which contributes to the criminalization of people.”).

³² See AMNESTY INTERNATIONAL, *supra* note 19; see also *Leaders of a Beautiful Struggle v. Balt. Police Dep’t*, No. 20-1495, 2021 U.S. App. LEXIS 18868 (4th Cir. June 24, 2021) (finding the Baltimore Police Department’s surveillance system violates the Fourth Amendment because persistent surveillance of outdoor movements invades people’s reasonable expectation of privacy).

³³ *Leaders of a Beautiful Struggle*, *supra* note 32; see also Amy Harmon, *As Cameras Track Detroit’s Residents, a Debate Ensues About Racial Bias*, NEW YORK TIMES (July 8, 2019), <https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html>.

³⁴ *Id.* at 24.

³⁵ *Id.* at 36 (explaining that “allowing the police to wield this power unchecked is anathema to the values enshrined in our Fourth Amendment.”).

³⁶ *Id.* at 4, 34.

³⁷ Jordan Williams, *Watchdog: Six Federal Agencies Used Facial Recognition Software to ID George Floyd Protesters*, THE HILL (June 29, 2021), <https://thehill.com/policy/technology/560805-watchdog-6-federal-agencies-used-facial-recognition-software-to-id-george>.

³⁸ See United States Government Accountability Office, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks* GAO-21-518 at 17-18 (June 2021), <https://www.gao.gov/assets/gao-21-518.pdf> (“Following the death of George Floyd while in the custody of the Minneapolis, Minnesota police department on May 25, 2020, nationwide civil unrest, riots, and protests occurred. Six



officers used facial recognition technology to cross-reference footage from protests with online images to identify Derrick Ingram, a Black activist who led a protest against police brutality in June 2020.³⁹ This resulted in over 50 police officers surrounding Ingram's apartment and according to him, officers deployed drones, police dogs and two helicopters for several hours before leaving.⁴⁰ While police surveillance and violence against Black protestors is not new,⁴¹ law enforcement's ability to identify protestors at the scale that facial recognition allows is a new and dangerous phenomenon. Law enforcement's unfettered use of this technology during protests risks chilling protected First Amendment activity of targeted groups which frequently include religious and ethnic minorities,⁴² and subjects them to a greater risk of police harm.⁴³

Overall, law enforcement's use of facial recognition technology creates a great risk that communities of color will increasingly be wrongly identified and subject to disparate criminal enforcement or a "surveillance state" where law enforcement monitors and tracks their movements, associations *en masse*, and chills their dissent.

agencies told us that they used images from these events to conduct facial recognition searches during May through August 2020 in order to assist with criminal investigations.").

³⁹ Aristos Georgiou, *Black Lives Matter Activist Hunted by NYPD Facial Recognition Technology*, NEWSWEEK (August 8, 2020), <https://www.newsweek.com/black-lives-matter-activist-hunted-facial-recognition-technology-1525335>.

⁴⁰ *Id.*; see also Adrienne Green, *The Room Where It Happened: Derrick Ingram is still shut inside the Hell's Kitchen apartment the police tried to invade*, NEW YORK MAGAZINE (May 25, 2021), <https://nymag.com/intelligencer/2021/05/derrick-ingram-nypd-standoff.html> (describing the 5 hour encounter and noting that though police later charged Ingram with third degree assault, it was reduced to a misdemeanor and eventually dismissed), and Katie Shepherd, *An artist stopped posting protest photos online to shield activists from police. Then, he was arrested.*, WASHINGTON POST (August 3, 2020), <https://www.washingtonpost.com/nation/2020/08/03/philadelphia-arrest-protest-photos/> (describing others targeted by police after police used facial recognition technology to identify them from footage derived from protests).

⁴¹ Katie Nodjimbadem, *The Long, Painful History of Police Brutality in the U.S.*, SMITHSONIAN MAGAZINE (July 27, 2017), <https://www.smithsonianmag.com/smithsonian-institution/long-painful-history-police-brutality-in-the-us-180964098/> ("Aggressive dispersion tactics, such as police dogs and fire hoses, against individuals in peaceful protests and sit-ins were the most widely publicized examples of police brutality in that era. But it was the pervasive violent policing in communities of color that built distrust at a local, everyday level.").

⁴² Klen Klippenstein, *Leaked FBI Documents Reveal Bureau's Priorities Under Trump*, THE YOUNG TURKS (August 8, 2019), <https://tvt.com/stories/4vZLCHuQrYE4uKagv0oyMA/mnzAKMpditZ7AcYLd5cRR> ("The documents, . . . reference a mysterious plan to mitigate the threat of 'Black Identity Extremists' with a program codenamed 'IRON FIST' involving the use of undercover agents.").

⁴³ See Facial Recognition Technology (I): Its Impact on Our Civil Rights and Liberties: Hearing Before the Committee on Oversight and Reform, 116th Cong., at 5–6 (2019) (statement of Andrew G. Ferguson, Professor of Law, University of the District of Columbia, David A. Clarke School of Law); *id.* at 7–9 (statement of Clare Garvie, Senior Associate, Georgetown University Law Center, Center on Privacy & Technology); *id.* at 9–11 (statement of Neema Singh Guliani, Senior Legislative Counsel, American Civil Liberties Union).



3. Law Enforcement's Expansive Use of Facial Recognition Technology is Largely Hidden, Allowing Police to Collect, Disclose, and Run an Individual's Personal Information Against Multiple Databases Without Their Knowledge, Implicating Privacy Concerns and Leaving Impacted Victims Unable to Contest or Remedy Resulting Harms

The opacity surrounding facial recognition technology—its creation, and the boundaries (or lack thereof) on its use—largely leaves the public in the dark about its use.⁴⁴ Additionally, because law enforcement agencies publicly report little to no information about officers' searches or use of technology, this also creates an obstacle in accessing information about the extent of law enforcement use of facial recognition technology.

At least one facial recognition technology company, Clearview AI, mines public platforms and/or photo databases, such as social media platforms and security footage for the datasets supporting its technology—all without the captured person's knowledge or consent.⁴⁵ A person's face could be used to create and train a facial recognition algorithm without them ever uploading a photo or consenting to its use.⁴⁶ When facial recognition technology is then shared with law enforcement agencies, police may run hundreds of thousands of searches for an identification, using any photo, against a broad range of available databases, without those in the database ever being informed of law enforcements' access to these photos, or use of such searches.⁴⁷ If the technology correctly identifies the individual, their identifying biometric information is then available for use across multiple law enforcement agencies, at the discretion of police, at the push

⁴⁴ See Feiner and Palmer, *supra* note 27; see also Andrew Wyrick, *NYPD sued for refusing to disclose records about facial recognition use*, DAILY DOT (July 21, 2020), <https://www.dailydot.com/debug/nypd-facial-recognition-law-suit-stop/>.

⁴⁵ Kashmir Hill, *The Secretive Company That Might End Privacy As We Know It*, NEW YORK TIMES, (Updated March 18, 2021), <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>; see also Drew Harwell, *This facial recognition website can turn anyone into a cop – or a stalker*, WASHINGTON POST (May 14, 2021), <https://www.washingtonpost.com/technology/2021/05/14/pimeyes-facial-recognition-search-secrecy/>; James Moore, *Facial recognition under scrutiny as Clearview AI's practices ruled illegal in Canada*, IFSEC GLOBAL (Feb. 16, 2021), <https://www.ifsecglobal.com/video-surveillance/facial-recognition-under-scrutiny-as-clearview-ais-practices-ruled-illegal-in-canada/> (the Canadian government ruled that Clearview's collection of biometric information from its citizens without their knowledge or consent is illegal).

⁴⁶ See e.g., Joseph Goldstein and Ali Walker, *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database.*, NEW YORK TIMES (August 1, 2019), <https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html>.

⁴⁷ Katie Canales, *Thousands of US police officers and public servants have reportedly used Clearview's controversial facial recognition tech without approval*, BUSINESS INSIDER (April 6, 2021), <https://www.businessinsider.com/clearview-ai-facial-recognition-thousands-police-departments-2021-4>; S.T.O.P. Condemns NYPD for 22K Facial Recognition Searches, SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT (Oct. 23, 2020), <https://www.stopspying.org/latest-news/2020/10/23/stop-condemns-nypd-for-22k-facial-recognition-searches>.



of a button.⁴⁸ The FBI revealed that it has access to over 400 million photos for face matching, including the driver's license databases of over fifteen states and passport application photos.⁴⁹ And just last year, Immigration and Customs Enforcement (ICE) used facial recognition technology to mine millions of drivers' license photos without the license-holders' knowledge, allowing for a broad targeting of immigrants.⁵⁰ Since few states restrict or prohibit ICE's access to personally identifying data, and the majority allow law enforcement officials to request similar searches against their driver's license databases,⁵¹ these intrusive warrantless searches occur in most states.⁵² The combination of facial recognition technologies incorporating publicly available photo datasets and law enforcement's unrestricted use of the technology exposes people to government identification and tracking⁵³ without their knowledge, and largely without independent oversight.⁵⁴

Additionally, there is very little data collected and made publicly available about the activities of individual law enforcement officers or agencies, including their use of facial recognition technology, that would permit public oversight. For example, data or information is not uniformly collected or shared publicly about officers or agencies' use of facial recognition technology to search databases and identify individuals.⁵⁵ The public does not know the demographic characteristics of persons searched, the justification for each search, what technology was used, how the search was conducted, or the outcomes of searches.⁵⁶ Subsequently, individuals

⁴⁸ Alfred Ng, *Police Say They Can Use Facial Recognition, Despite Bans*, THE MARKUP (January 28, 2021), <https://themarkup.org/news/2021/01/28/police-say-they-can-use-facial-recognition-despite-bans> (explaining that the current patchwork of local bans on facial recognition technology still allows law enforcement agencies to easily share information gathered via facial recognition technology).

⁴⁹ U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-267, *FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY* (May 2016), <https://www.gao.gov/assets/680/677098.pdf>.

⁵⁰ Catie Edmundson, *ICE Used Facial Recognition to Mine State Driver's License Databases*, NEW YORK TIMES (July 9, 2017), <https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html>.

⁵¹ See Testimony Before the Comm. on Oversight and Reform, House of Representatives, *Facial Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains* GAO-19-579T at 2, 5-6 (2019) (statement of Gretta L. Goodwin), <https://www.gao.gov/assets/gao-19-579t.pdf> (since 2011 the FBI has logged more than 390,000 facial recognition searches of federal and local databases, including state DMV databases).

⁵² See Edmundson, *supra* note 50.

⁵³ Ryan Mac et al., *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA*, BUZZFEED NEWS (February 27, 2020), <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement>.

⁵⁴ Clare Garvie, *Garbage In, Garbage Out: Face Recognition On Flawed Data*, GEORGETOWN CENTER ON LAW AND PRIVACY (May 16, 2019), <https://www.flawedfacedata.com> ("There are no rules when it comes to what images police can submit to face recognition algorithms to generate investigative leads.").

⁵⁵ See *supra* note 32.

⁵⁶ See Garvie, *supra* note 54 ("The NYPD made 2,878 arrests pursuant to face recognition searches in the first 5.5 years of using the technology [...] Florida law enforcement agencies . . . run on average 8,000 searches per month of the Pinellas County Sheriff's Office face recognition system, [but] many other agencies do not keep close track of how many times their officers run face recognition searches and whether these searches result in an arrest.").



have little room to understand the extent that facial recognition played in law enforcement activity, recourse to challenge its use, or the ability to contest abuses or errors.⁵⁷

Law enforcement's unfettered use of facial recognition technology allows for an expansive reach that raises serious privacy concerns because it allows law enforcement officials to collect, disclose, and use an individual's personal information from multiple databases without their knowledge.⁵⁸ As explained above, the burden of this harm falls disproportionately on Black and Brown communities.

4. Law Enforcement Officers and Agencies Should Not Be Permitted to Use Facial Recognition Technology

In the wake of the murder of George Floyd and the resulting outcry, much remains to be done to end systemic racism⁵⁹ and police violence in our public safety systems. Law enforcement's use of facial recognition technology cannot be addressed without a reckoning of the systemic racism and police violence in our current public safety systems in the United States. Until we transform our public safety systems, law enforcement's use of facial recognition technology will only exacerbate the systemic harm that officers and agencies cause to communities of color even without such technology.

Recognizing these dangers, multiple cities across the country⁶⁰ have rightfully implemented a complete ban on law enforcement's use of facial recognition technology.⁶¹ San Francisco's "Stop Secret Surveillance Ordinance" warned of its propensity to "exacerbate racial injustice and threaten our ability to live free of continuous government monitoring."⁶² Similarly, Maine enacted the country's strongest statewide facial recognition law, banning the use of the technology in most areas of government, and explicitly applying the ban to law enforcement

⁵⁷ Aaron Mak, Facing Facts: A case in Florida demonstrates the problems with using facial recognition to identify suspects in low-stakes crimes, SLATE (January 25, 2019), <https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html>.

⁵⁸ See e.g., Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921 (2002) (outlining privacy protections for citizens' personal information); see also GAO Report, *supra* note 51 (discussing the privacy implications of federal agencies use of facial recognition technology).

⁵⁹ See sources cited *supra* note 8 (listing multiple DOJ investigation and federal and state court decisions, all finding racially discriminatory police practices in police departments across the country).

⁶⁰ David Gutman, *King County Council bans use of facial recognition technology by Sheriff's Office, other agencies*, SEATTLE TIMES (June 1, 2021), <https://www.seattletimes.com/seattle-news/politics/king-county-council-bans-use-of-facial-recognition-technology-by-sheriffs-office-other-agencies/>.

⁶¹ *Ban Facial Recognition Map: Bans*, FIGHT FOR THE FUTURE, <https://www.banfacialrecognition.com/map/>.

⁶² Sarah Emerson, *San Francisco Bans Facial Recognition Use by Police and the Government*, VICE (May 14, 2019), <https://www.vice.com/en/article/wjvxxb/san-francisco-bans-facial-recognition-use-by-police-and-the-government>.



agencies.⁶³ At least 7 states have prohibited some law enforcement use⁶⁴ and multiple other jurisdictions have imposed at least a moratorium on law enforcement's use of facial recognition technology.⁶⁵ Amazon, Microsoft, and IBM, stopped selling facial recognition technology to law enforcement agencies.⁶⁶ These governmental and private actions to cease supporting law enforcement use of facial recognition were taken due to concerns regarding the legitimate dangers of such use. The federal government should follow suit.

Conclusion

Allowing law enforcement agencies to use this invasive and faulty technology threatens to exacerbate, and effectively ignores the documented dangers of systemic racism in America's law enforcement.⁶⁷ We must not equip law enforcement with the tools to weaponize data and technology against our communities, particularly when such use reinforces racial bias and discriminatory conduct. We urge this Subcommittee to address police accountability, brutality, and the over-policing of Black and Brown communities before authorizing law enforcement use of facial recognition technology. Attempts to address law enforcement's use of facial recognition technology must confront and first end racially disparate policing practices that have been found in agencies nationwide and the police violence disproportionately experienced by communities of color.

Thank you for considering these recommendations. We look forward to continuing to work with this Subcommittee on this critical issue of law enforcement use of facial recognition technology. If you have any questions, please contact Katurah Topps, Policy Counsel, at

⁶³ L.D. 1585 (H.P. 1174), An Act to Increase Privacy and Security by Regulating the Use of Facial Surveillance Systems by Departments, Public Employees and Public Officials (June 17, 2021) <http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=HP1174&item=2&snum=130>.

⁶⁴ Julie Carr Smyth, *States Push Back Against Use of Facial Recognition by Police*, U.S. NEWS AND WORLD REPORT (May 5, 2021), <https://www.usnews.com/news/politics/articles/2021-05-05/states-push-back-against-use-of-facial-recognition-by-police>; Susan Crawford, *Facial Recognition Laws Are (Literally) All Over the Map*, WIRED (Dec. 16, 2019), <https://www.wired.com/story/facial-recognition-laws-are-literally-all-over-the-map/> ("California joined New Hampshire and Oregon in prohibiting law enforcement from using facial recognition and other biometric tracking technology in body cameras. Illinois passed a law that permits individuals to sue over the collection and use of a range of biometric data, including fingerprints and retinal scans as well as facial recognition technology. Washington and Texas have laws similar to the one in Illinois, but don't allow for private suits.").

⁶⁵ *Ban Facial Recognition Map: Other Laws, State & Local*, FIGHT FOR THE FUTURE, <https://www.banfacialrecognition.com/map>.

⁶⁶ Rebecca Heilweil, *Big tech companies back away from selling facial recognition to police. That's progress.*, VOX (June 11, 2020), <https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police>.

⁶⁷ Emily Kwong, *Short Wave: Why Tech Companies Are Limiting Police Use of Facial Recognition*, NATIONAL PUBLIC RADIO (Feb. 18, 2021), <https://www.npr.org/2021/02/17/968710172/why-tech-companies-are-limiting-police-use-of-facial-recognition>.



ktopps@naacpldf.org or (212) 965-2200, or Puneet Cheema, Manager of the Justice in Public Safety Project at pcheema@naacpldf.org or (646) 574-5666.

Sincerely,

A handwritten signature in black ink, appearing to read "Lisa Cylar Barrett", written over a horizontal line.

Lisa Cylar Barrett, Director of Policy

Puneet Cheema, Manager of Justice in Public
Safety Project

Katurah Topps, Policy Counsel

cc: Members of the Subcommittee on Crime, Terrorism, and Homeland Security

QUESTIONS FOR THE RECORD

Questions for the Record from Rep. Louie Gohmert for Ms. Gretta L. Goodwin, Director,
Homeland Security and Justice, U.S. Government Accountability Office

1. In your written testimony, it states the following regarding GAO's findings: "Three agencies reported using it (that is, facial recognition technology) on images of the U.S. Capitol attack on January 6, 2021. Agencies said the searches used images of suspected criminal activity." Later on in your written testimony it states, "The three agencies reported using the technology to generate investigative leads for criminal investigations."
1. Can you explain these findings in a bit more detail for the Committee? Were the results used to obtain warrants? If so, were the courts apprised of the failure rate of FRT?
2. Can you describe the internal rules and regulations that govern the use of facial recognition technology in the three agencies which reported using facial recognition technology on images of individuals at the U.S. Capitol on January 6, 2021?
3. Concerning the U.S. Capitol Police's use of Clearview AI to generate investigative leads from January 6th, is it true that unsuspecting Americans, many of whom simply came to their nation's Capital to protest vote deprivation were subjected, without their consent and without warrants, to having their online accounts like Facebook and Instagram scoured by the Capitol Police or other Federal agencies via a 3rd party (Clearview AI)?

Questions for the Record from Rep. Louie Gohmert for Mr. Brett Tolman, Executive Director, Right on Crime

1. In your written testimony, you state the following: “Also discomforting are the sources of the photos supporting this facial recognition technology. In addition to drawing on pictures secured through the criminal justice process, the government utilizes millions of photos of law-abiding individuals collected for driver’s licenses and passports. Private technology companies that contract with law enforcement have harvested billions of photos posted by unsuspecting users on platforms such as Facebook, YouTube, and even Venmo. This collection is an unprecedented invasion of privacy that places enormous, undue control in the hands of the government and Big Tech, two entities not always known for their light touch or responsible use of power.”
 1. Can you explain to us exactly what Clearview AI was likely to have provided the U.S. Capitol Police and how “the process” works?
 2. Regarding any photos that were harvested from online services like Facebook or Instagram, would users have been warned that their information would be shared by a private technology company with law enforcement entities?
2. In your written testimony, you further state: “Our Founding Fathers deliberately and prudently enshrined in the Bill of Rights proscriptions on the wanton search of Americans as a necessary bulwark for freedom. It is hard to square these notions and protections with the unfettered use of a technology that can instantaneously reveal an individual’s identity as well as potentially their associations and prior movements. The unrestricted use of facial recognition bears little difference to allowing police to collect fingerprints or DNA from anyone and everyone they come across, an abuse that we clearly do not, and should not, tolerate.”
 1. How can we ensure that Americans’ Constitutional rights won’t continue to be trampled by facial recognition technology?
 2. Are you familiar with Texas’ biometric privacy statute enacted in 2009?
 - a. If yes, do you think it is good model legislation for the nation?
 - b. What improvements to the Texas biometric privacy statute would you suggest?

Questions for the Record from Rep. Louie Gohmert for Ms. Kara Frederick, Research Fellow, Center for Technology Policy, The Heritage Foundation

1. Are you familiar with Texas' biometric privacy statute enacted in 2009?
 - a. If yes, do you think it is good model legislation for the nation?
 - b. What improvements to the Texas biometric privacy statute would you suggest?

Questions for the Record from Rep. Louie Gohmert for Ms. Gretta L. Goodwin, Director,
Homeland Security and Justice, U.S. Government Accountability Office

In your written testimony, it states the following regarding GAO's findings: "Three agencies reported using it (that is, facial recognition technology) on images of the U.S. Capitol attack on January 6, 2021. Agencies said the searches used images of suspected criminal activity." Later on in your written testimony it states, "The three agencies reported using the technology to generate investigative leads for criminal investigations."

1. Can you explain these findings in a bit more detail for the Committee? Were the results used to obtain warrants? If so, were the courts apprised of the failure rate of FRT?

We can explain these findings in more detail; however, the response would require the inclusion of sensitive information. As agreed to with your office, we will provide a response in a format appropriate for sensitive information.

As part of our June 2021 report on law enforcement use of facial recognition technology, we surveyed 42 federal agencies that employed law enforcement officers.² The purpose of this report was to understand the 'lay of the land' regarding facial recognition technology that was owned and used by the law enforcement community. As such, we did not review how agencies used the results of individual facial recognition searches. For example, we did not determine whether agencies used the results of searches related to the U.S. Capitol attack to obtain warrants.

2. Can you describe the internal rules and regulations that govern the use of facial recognition technology in the three agencies which reported using facial recognition technology on images of individuals at the U.S. Capitol on January 6, 2021?

Federal agency collection and use of personal information, including face images, is generally governed primarily by two laws: the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002. The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems

²GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, GAO-21-518 (Washington D.C.: June 3, 2021).

of records.³ 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 in the Federal Register. According to 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 Act. Further, the E-Government Act of 2002 requires that agencies conduct Privacy Impact Assessments before developing or procuring information technology (or initiating a new collection of information) that collects, maintains, or disseminates personal information.⁴ 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 Privacy Impact Assessments 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. Furthermore, according to OMB officials, the Privacy Act and OMB Circular A-130 generally provide that agencies must ensure that privacy requirements apply to systems operated by contractors or other entities on behalf of the Federal Government, which could include facial recognition service providers.

As discussed earlier, the purpose of our June 2021 report was to understand the 'lay of the land' regarding facial recognition technology that was owned and used by the law enforcement community. As such, we did not review the 42 agencies' internal rules and policies that govern their use of facial recognition technology. However, in the past, we have reviewed the U.S. Customs and Border Protection's use of facial recognition at U.S. ports of entry. For example, in September 2020, we reviewed the extent to which U.S. Customs and Border Protection incorporated the Fair Information Practice

³The Privacy Act defines "agency" as any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency. 5 U.S.C. § 552(f)(1).

⁴For the purposes of the E-Government Act, an agency means an Executive branch agency. See 5 U.S.C. § 3701(1).

Principles into its Biometric Entry-Exit Program, a Department of Homeland Security program that uses traveler photos to verify the identity of travelers entering or exiting U.S. ports of entry.⁵

3. **Concerning the U.S. Capitol Police's use of Clearview AI to generate investigative leads from January 6, is it true that unsuspecting Americans, many of whom simply came to their nation's Capital to protest vote deprivation were subjected, without their consent and without warrants, to having their online accounts like Facebook and Instagram scoured by the Capitol Police or other Federal agencies via a 3rd party (Clearview AI)?**

The U.S. Capitol Police reported using Clearview AI's facial recognition technology on images from the U.S. Capitol attack to help generate investigative leads. Although the U.S. Customs and Border Protection and Department of State's Bureau of Diplomatic Security reported using Clearview AI in the past, these agencies did not report using the technology on images from the U.S. Capitol attack.

Representatives of Clearview AI told us that their system includes a database of roughly 3 billion images publicly available on the public internet. For example, according to Clearview AI, it may gather images publicly available on websites such as Facebook. Although Clearview AI told us that it collects publicly available photos from the internet for facial recognition searches, we did not specifically ask whether images from the U.S. Capitol attack were included in its database.

⁵GAO, *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, GAO-20-568 (Washington, D.C.: September 2, 2020).

Tolman Facial Recognition Responses

Can you explain to us exactly what Clearview AI was likely to have provided the U.S. Capitol Police and how “the process” works?

Part of the problem we face is that it’s unclear how exactly the federal government has come to rely on facial recognition technology and whether it truly has policies in place deserving of even being called a “process.” Agencies typically reveal little about its use, such as that it simply is utilized to generate “investigative leads,” with little further elaboration. We are instead left to make educated guesses as to how agencies, such as the U.S. Capitol Police, are utilizing this technology.

Clearview AI and its competitors retain vast databases of images harvested from publicly available sources. In the age of social media, there is no shortage of personal information easily accessible on the web, even relating to Americans who have never placed it there themselves. Law enforcement agencies turn to private facial recognition companies when they have an unidentified suspect whom they either cannot identify through government databases or believe it would be easier to do so with private assistance. These technology companies are then able to run an image of the unidentified individual through their own massive database with a search algorithm that seeks possible matches based on various biometric identifiers. If and when a possible match is found, the company is typically able to provide information such as a probable name and potentially other details on that individual to law enforcement.

Regarding any photos that were harvested from online services like Facebook or Instagram, would users have been warned that their information would be shared by a private technology company with law enforcement entities?

Not in any meaningful way. At this point, we are all quite familiar with the lengthy, at times seemingly indecipherable, legal terms that flash across our computer screen and require our consent before we’re able to access a given online service. Many of these companies that collect Americans’ data include language detailing the possible uses of that information, which typically includes law enforcement access. Anyone diligent enough to read through that disclaimer, possibly with the assistance of counsel, will be advised of those uses. However, even then, to call this consent is something of a fiction. Few people are willing to sacrifice the utility of these programs—many of which have few real competitors or replacements—to safeguard those rights, even if they do not like the prospect of signing away that privacy. Recognizing these limitations to consent, Congress has previously considered barring discrimination by these companies against individuals who do not consent to the use of their biometric identifiers.

How can we ensure that Americans’ Constitutional rights won’t continue to be trampled by facial recognition technology?

Right now, we are counting on the good intentions and competence of government actors, and that is a recipe for abuse. Instead, we need congressional action to protect the privacy interests of Americans. This should have two primary components: limitations on the collection and use of biometric identifying information by private actors and law enforcement alike, and robust measures for transparency and accountability. States such as Texas and Illinois have led the way with biometric privacy laws that provide a foundation off of which Congress could build a framework to protect all Americans. These laws address the supply side of the issue—private

collection and use—while also constraining demand by requiring law enforcement to secure a warrant. In so doing, they preserve the ability of law enforcement to harness this technology on behalf of public safety, without jeopardizing the rights of Americans. These state laws, however, only constrain private actors, which leaves government still able to operate facial recognition databases in-house with relatively few limitations. Although there are legitimate reasons for the government to collect and retain biometric identifiers—driver’s licenses, for example—Congress could nevertheless develop rules to limit which additional information government actors collect as well as under which circumstances they may utilize facial recognition searches on these databases.

Are you familiar with Texas’ biometric privacy statute enacted in 2009?

a. If yes, do you think it is good model legislation for the nation?

It’s a great start. It places significant limitations on the private collection and use of individuals’ biometric identifying information, while also requiring law enforcement to secure a warrant in order to access this information.

b. What improvements to the Texas biometric privacy statute would you suggest?

There are two provisions that Texas may wish to consider borrowing from Illinois’ Biometric Information Privacy Act. First, Illinois’ law grants individuals the right to sue in defense of their privacy rights. This establishes that the individual is indeed harmed by the violation of their own privacy and ensures that they are not reliant on government to defend themselves. Second, the Illinois law includes protections not just for biometric identifiers—as Texas does—but “biometric information.” This latter category is more expansive and may prove necessary as algorithms become more advanced and able to identify individuals based on a larger set of information. Likewise, Texas may wish to consider adding a warrant requirement for government actors to conduct facial recognition searches in criminal investigations generally (not just from commercial databases), as states like Massachusetts have done.

I am familiar with Texas' biometric privacy statute from 2009.

- a. In terms of its suitability as model legislation for the nation, the existing Texas law can be updated to promote transparency regarding the data-sharing relationships between commercial entities and state, local, and federal governments. Public reports that detail when and how government entities outsource facial recognition capabilities and biometric collection to the private sector can help constrain misuse by both parties.
- b. In practice, creating safeguards to mitigate abuse by commercial actors (at times on behalf of the government) can look like:
 - A provision that commercial actors publicize annual transparency reports on government requests for biometric data and whether that disclosure occurred.
 - The stipulation that in the event of a biometric data-sharing transaction between commercial and government entities, the full suite of Fair Information Practice Principles (FIPPs)—some of which are already enshrined in the Texas law—applies to the handling of this biometric data.¹
 - A provision that commercial actors publicize annual transparency reports on how they collect, store, and share biometric data both within the company (e.g. what technical guardrails are in place) and among other commercial and non-government actors.

¹According to the U.S. Department of Homeland Security, these principles consist of: “Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing.” *United States Department of Justice*, “Overview of the Privacy Act of 1974 (2020 Edition),” 2020, p.1, <https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition> (accessed August 9, 2021) and *United States Department of Homeland Security*, “Privacy Policy Guidance Memorandum,” December 29, 2008, p.1, <https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf> (accessed August 9, 2021).