GEORGETOWN LAW
Center on Privacy & Technology

Statement of Clare Garvie
Senior Associate, Center on Privacy & Technology at Georgetown Law

Before the

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

Hearing on

Facial Recognition Technology (Part 1): Its Impact on Our Civil Rights and Liberties

Wednesday, May 22, 2019

For more information, contact Clare Garvie at clare.garvie@georgetown.edu

Introduction and Summary

Chairman Cummings, Ranking Member Jordan, and distinguished members of the Committee, thank you for inviting me here today. I am Clare Garvie, a senior associate at the Center on Privacy & Technology at Georgetown Law. I appreciate the opportunity to offer testimony regarding police use of face recognition technology, and its impact on our civil rights and liberties.

I am an expert in how automated face recognition is used by law enforcement agencies across the United States. Staff at the Center on Privacy & Technology have been researching and advocating for restrictions on face recognition for close to a decade. I personally have been researching face recognition and its risks to privacy, civil rights, and civil liberties for the past four years. In that time I have FOIA'd hundreds of federal, state, and local agencies and read close to 20,000 pages of government records on how the technology works and is used. I have been the lead author of three studies into police use of face recognition technology, and conduct trainings on a routine basis for public defenders and advocates on how the technology is used within our criminal justice system.

Based on this expertise I can state with confidence: Face recognition presents a unique threat to our civil rights and liberties protected by the U.S. Constitution. The Committee convenes this hearing at an important time, just as the city of San Francisco has voted to ban use of automated face recognition, in recognition not only of its technical unreliability, but also of its potential to exacerbate racial injustice. Numerous other communities around the country also are considering whether to allow or reject face recognition technology, and grappling with the many problems with this technology that recent research—including my own—has exposed.

This testimony makes five main points:

1. **Face recognition gives law enforcement a power they've never had before.** This power calls into question our Fourth Amendment expectations of privacy and the rights afforded to us by the First Amendment. The Supreme Court in *Carpenter v. United States* noted that for the government to "secretly monitor and catalogue every single movement" of someone across time and space violates our expectations of privacy protected by the Fourth Amendment. Face recognition technology enables

precisely this type of monitoring. The Supreme Court held in *NAACP v. Alabama, Talley v. California,* and other cases that the First Amendment protects the right to anonymous speech and association. Face recognition technology threatens these protections.

For example, rather than respecting anonymous protesting, the Baltimore County Police Department used face recognition, in conjunction with social media monitoring, to keep tabs on protests following the death of Freddie Gray in police custody in 2015. Photos uploaded to social media sites from protest locations were run through Maryland's face recognition technology to enable police officers to arrest people directly from the crowd.

2. **Face recognition is flawed, and the consequences of its mistakes will be borne disproportionately by African American communities.** Communities of color are disproportionately the targets of police surveillance, face recognition included. People of color are also disproportionately enrolled in police face recognition databases. And studies continue to show that the accuracy of face recognition systems varies depending on the race and gender of the person being searched. Face recognition makes mistakes, and risks making *more* mistakes—more misidentifications—of African Americans.

3. **Left unchecked, current police face recognition practices threaten Constitutional guarantees to due process.** In the absence of rules and transparency, police submit what can only be described as "garbage" data into face recognition systems, expecting valuable leads in return. Research shows they also at times skip traditional identification procedures and go straight to arresting a suspect based on face recognition leads, raising serious questions about accuracy and the potential for misidentification. And defendants are left completely in the dark.

   In a study released last week, I uncovered particularly egregious examples of this practice, including a case where the NYPD submitted a photo of Woody Harrelson to its face recognition system to search for an unknown suspect in a beer theft, thinking the two bore a resemblance.[1]

[1] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data* (May 16, 2019), https://www.flawedfacedata.com/ [hereinafter *Garbage In, Garbage Out*].

4. **Police use of face recognition continues to become more pervasive and advanced, and the law does little to protect against the risks it poses.** More than half of all American adults are enrolled in a face recognition network.[2] And for millions of Americans in major cities across the United States, face surveillance may be an imminent reality. In another study released last week, my research found that Chicago and Detroit have both acquired powerful face surveillance tools designed to operate on 100 or more cameras—with little or no public transparency or oversight. Orlando, Washington, D.C., and New York City are also trialling face surveillance systems.[3]

   For the vast majority of police face recognition applications, the law is silent. If it remains silent, we can only expect the technology to become more widespread and advanced.

5. **We need to hit the pause button on face recognition.** In light of the problems outlined above, federal, state, and local governments should enact moratoria on the use of the technology for law enforcement purposes. These moratoria will offer some jurisdictions the opportunity to ban the technology altogether; these jurisdictions will be amply justified in their actions. For others, I recommend a combination of targeted bans, strict court oversight and regulation, transparency and public reporting, and provisions to publicly test the accuracy and bias of algorithms used for law enforcement. A few years ago I thought that regulation of this technology would be enough to address the risks it raised. Today, in light of what I have learned about how powerful, pervasive, and susceptible to abuse face recognition is, I think we need to hit the pause button.

1. Face recognition presents a unique threat to privacy and civil rights.

As many communities are realizing, automated face recognition presents a unique threat to privacy and civil rights. This technology gives law enforcement a power it has never had before. That power threatens some of

[2] Clare Garvie, Alvaro M. Bedoya, & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, (Oct. 18, 2016), https://www.perpetuallineup.org/findings/deployment [hereinafter *The Perpetual Line-Up*].

[3] Clare Garvie & Laura Moy, *America Under Watch: Face Surveillance in the United States* (May 16, 2019), https://www.americaunderwatch.com [hereinafter *America Under Watch*].

our society's core freedoms. The technology itself also suffers from critical technical flaws and bias problems and, as a consequence, the failures of the technology will disproportionately harm communities of color. Making matters worse, some entities misuse and abuse this technology, and often shroud their possession and use of it in secrecy.

A. Face recognition gives law enforcement a power it has never had before.

Face recognition is already extremely powerful with the potential to become even more so, granting law enforcement agencies abilities they have never had before. Face recognition is distinct from past law enforcement surveillance technologies in at least three ways: (1) it is remote and secret; (2) it relies on existing, massive databases that have been built from the routine behavior of law-abiding citizens; and (3) once it is implemented, it is virtually impossible for people to opt out of being recognized and surveilled.

Remote and secret biometric surveillance. First, face recognition enables biometric surveillance for the first time ever—the scanning of groups of people remotely and in secret to identify them. Law enforcement cannot secretly fingerprint a crowd of people from across the street. They cannot conduct DNA searches in this capacity either. It is impossible—and illegal—for police to walk through a crowd of people, secretly pick-pocketing them to identify them from their driver's license photo. But with face recognition technology, law enforcement has gained the ability to scan people's faces and ID them—from remote locations and in secret—potentially of many people at one time.

This ability threatens to fundamentally change the nature of America's public spaces. The Supreme Court in *Carpenter v. United States*, examining the degree to which Fourth Amendment protections extended to digital cell-site location information, stated: "A person does not surrender all Fourth Amendment protection by venturing into the public sphere."[4] The Court noted that for the government to "secretly monitor and catalogue every single movement" of someone across time and space risked opening "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual

[4] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018)

associations'" and breaching our society's expectation about what law enforcement can and should be able to do.[5]

Face recognition opens that same, intimate window into our lives. But unlike with the cell phones that create the cell-site location information addressed in *Carpenter*, we cannot choose to leave our faces at home.

Biometric databases of most American adults. Second, the massive databases that enable identification via face recognition already include a majority of American adults. Most of the largest face photograph databases on file with a federal or state agency—passports, visas, driver's licenses—are now face recognition databases. And these databases are increasingly open to criminal justice searches by external law enforcement agencies. So while most Americans are not enrolled in criminal fingerprint or DNA databases, most of us *are* now enrolled in de facto criminal face recognition databases.

In fact, the FBI now has the ability to run face recognition searches against driver's license photos from at least 18 states.[6] State law enforcement agencies have access to driver's license face recognition databases in at least 31 states, constituting more than 54% of American adults.[7]

This represents a sweeping expansion of law enforcement access to personal data. Never before have state and local police departments, or the FBI, had the ability to run biometric searches against a majority of their—or another—state's citizens when conducting routine investigations.

[5] *Id.* (quoting United States v. Jones, 565 U.S. 400, 415 (Sotomayor, J., concurring)).
[6] *See* House Committee on Oversight and Reform, *Committee to Review Law Enforcement's Policies on Facial Recognition Technology* (Mar. 22, 2017), https://republicans-oversight.house.gov/hearing/law-enforcements-use-facial-recognition-technology/ (listing the FBI Memoranda of Understanding affording it the ability to run or request searches of 18 states' driver's license databases).
[7] Garvie, Bedoya & Frankle, *The Perpetual Line-Up* at Figure 6 (estimating that just under 50% of all American adults were in a face recognition database accessible to law enforcement, and noting that law enforcement at that time had access to driver's license photos in at least 26 states). Since the publication of that report, the Center on Privacy & Technology has confirmed that Alaska, Idaho, Indiana, New Jersey, South Dakota, and Wisconsin have DMV face recognition systems that are accessible to law enforcement. Vermont has since terminated its system.

In fact, Americans have repeatedly rejected efforts to create national biometric databases, citing concerns about precisely this type of use.[8] President Reagan is reported to have likened proposals to create a national ID system in 1981 to the biblical "mark of the beast."[9] President Clinton dismissed a similar measure because the idea invoked "Big Brother."[10] And despite sponsors' attempts to distinguish the REAL ID Act of 2005 from a biometric ID system, after its passage 23 states passed laws prohibiting their agencies from complying with the Act or funding its adoption, many due at least in part to concern over federal access to, and misuse of, state residents' personal information.[11]

No option to opt-out. Third, once face recognition is implemented, it becomes virtually impossible for people to unenroll themselves or opt out of being recognized and monitored by law enforcement agencies that possess this capability.

It is not just a question of refraining from criminal activity to avoid enrollment in a mugshot database; most Americans have enrolled themselves by obtaining a driver's license or state ID card, likely without their knowledge. And most of us do not consider obtaining a license to drive to be optional—for many Americans this is a requirement to hold down a job, take our children to school, and engage in myriad other necessities like grocery shopping and going to a doctor appointment. There is no meaningful choice to opt-out.

[8] A summary of these sentiments is provided by Alex Nowrasteh, *5 Reasons Why America Should Steer Clear of a National ID Card*, Fox News (March 9, 2010), https://www.foxnews.com/opinion/5-reasons-why-america-should-steer-clear-of-a-national-id-card ("...it would treat every American like a criminal by requiring them to enter their most intimate and personal data into a government database.").

[9] *See* Stephen Moore, *The National ID Card: It's Baaack!,* Cato Institute (Sept. 23, 1997), https://www.cato.org/publications/commentary/national-id-card-its-baaack.

[10] *See* ACLU, *Broad Coalition Urges President Obama and Congress to Oppose Biometric National ID* (Apr. 13, 2010), https://www.aclu.org/press-releases/broad-coalition-urges-president-obama-and-congress-oppose-biometric-national-id.

[11] *See, e.g.* Utah Uniform Driver License Act Section 104.5: Legislative finding -- Prohibition on implementing REAL ID Act (finding that the Act was "inimical to the security and well-being" of the state. The 23 states were: Arizona, Arkansas, Colorado, Georgia, Hawaii, Idaho, Illinois, Louisiana, Maine, Michigan, Minnesota, Missouri, Montana, Nebraska, Nevada, New Hampshire, North Dakota, Oklahoma, Pennsylvania, South Carolina, Tennessee, Utah, Virginia, Washington State.).

Moreover, this is the human face—something that is almost always exposed and that is critical to social identity and interaction. If people want to opt out of cell phone tracking, they can leave their phone at home. You cannot leave your face at home. You also cannot walk around the street wearing a mask unless it is Halloween or the dead of winter. Not only would this be impractical, it likely would invite more, not less scrutiny. In many states it could also lead to a fine or imprisonment.[12]

B. Face recognition threatens basic freedoms.

Because face recognition is such a powerful tool, it threatens some of our basic freedoms. Researchers who study human behavior have, in the past few years, demonstrated something that many consider intuitive: Government surveillance does in fact chill speech.[13] Alarmingly, this chilling effect falls disproportionately on those who hold—and would express—viewpoints they believe to be unpopular or divergent from majority opinion.[14]

Law enforcement agencies themselves have recognized this as a risk inherent to using face recognition. A Privacy Impact Assessment (PIA) authored by The International Justice and Public and Safety Network (Nlets) in 2011, examining face recognition used in conjunction with driver's license databases, stated:

> *"The public could consider the use of facial recognition in the field as a form of surveillance . . . . The potential harm of surveillance comes from its use as a tool for social control. The*

[12] *See, e.g.,* Minn. Stat. § 609.735 ("A person whose identity is concealed by the person in a public place by means of a robe, mask, or other disguise, unless based on religious believes, or incidental to amusement, entertainment, protection from weather, or medical treatment, is guilty of a misdemeanor."); *see, e.g.,* N.C. Gen. Stat. § 14-12.8 ("No person or persons shall in this State, while wearing any mask, hood or device whereby the person, face or voice is disguised so as to conceal the identity of the wearer, enter, or appear upon or within the public property of any municipality or county of the State, or of the State of North Carolina.").

[13] Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 Journalism & Mass Communication Quarterly 296 (2016); Elizabeth Stoycheff, *Mass Surveillance Chills Online Speech Even When People Have "Nothing to Hide,"* Slate (May 3, 2016), http://www.slate.com/blogs/future_tense/2016/05/03/mass_surveillance_chills_online_speech_even_when_people_have_nothing_to.html.

[14] *Id.*

> *mere possibility of surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition."*[15]

For these reasons, the document's authors recommended that face recognition never be used in the field as a "ubiquitous system that is covertly deployed and used to identify people without their consent or knowledge."[16] Rather, when deployed in the field it should only be used to identify individuals already detained by law enforcement and under policies restricting its use to specific instances of criminal conduct.

But no laws, and few law enforcement policies, have adopted these restrictions.

As a consequence, face recognition *has* been used to monitor First Amendment-protected activity. After the death of Freddie Gray in police custody in 2015, the Baltimore County Police Department employed face recognition, in conjunction with the social media monitoring tool Geofeedia, to keep tabs on the ensuing protests.[17] Photos uploaded to social media sites from protest locations were run through Maryland's face recognition technology to enable police officers to arrest people directly from the crowd.[18]

As use of face recognition technology in public spaces continues to expand, the impact on our public and political discourse could be devastating. Will you attend a protest, a pro-choice march, or a gun rights rally, if you know your face could be scanned?

[15] Nlets, *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field*, 17 (June 30, 2011), *available at* https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf (internal cites omitted. The PIA was drafted by the Nlets Facial Recognition Workgroup, composed of practitioners from the FBI, New Jersey State Police, Illinois State Police, North Carolina DMV, Pinellas County Sheriff's Office, Delaware State Police, Automated Regional Justice Information System, Oregon State Police, New York State DMV, County of Cumberland District Attorney's Office, and the Chicago High Intensity Drug Trafficking Area.)

[16] *Id.*

[17] Geofeedia, *Baltimore County Police Department and Geofeedia Partner to Protect the Public During Freddie Gray Riots* (obtained by ACLU Northern California Oct. 11, 2016), *available at* https://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf.

[18] *Id.*

C. Face recognition is inaccurate and biased.

Not only is face recognition powerful and threatening to our basic freedoms, but it also is flawed and biased. Television programs and movies would have us believe that face recognition can positively identify an individual with perfect accuracy from any photograph—that even low-resolution photos can magically be "enhanced" by sophisticated software programs so that law enforcement can locate suspects with complete confidence that they are tracking the right person. But that fiction is far from the reality. In addition, the mistakes that face recognition technology makes will be borne disproportionately by African-American communities.

Face recognition technology is imperfect. Face recognition makes mistakes, and may well never be perfect. The accuracy of a face recognition system is highly dependent on the quality of the photographic evidence provided it. Poor quality photos—grainy surveillance footage, poor lighting, faces that are obscured or turned away from the camera—will generally produce less reliable results than high quality face photographs.[19] Heavily edited photos, or just plain wrong information will also produce less accurate results, as discussed below.[20]

And when face recognition fails to identify the correct person, it may *misidentify* the *wrong* person—an error that could have disastrous consequences for that person. For example, just last month, Sri Lankan authorities relying on face recognition technology mistook an American college student for a woman suspected of participating in the Easter bombings.[21] As a result, the student received numerous death threats. "So many people just calling for me to be hanged," she said.[22] And although the student's name was quickly cleared, and most of the consequences she suffered were emotional in nature, a case of misidentification in a criminal

[19] For a more complete discussion of this, *see* Garvie, Bedoya & Frankle, *The Perpetual Line-Up*.

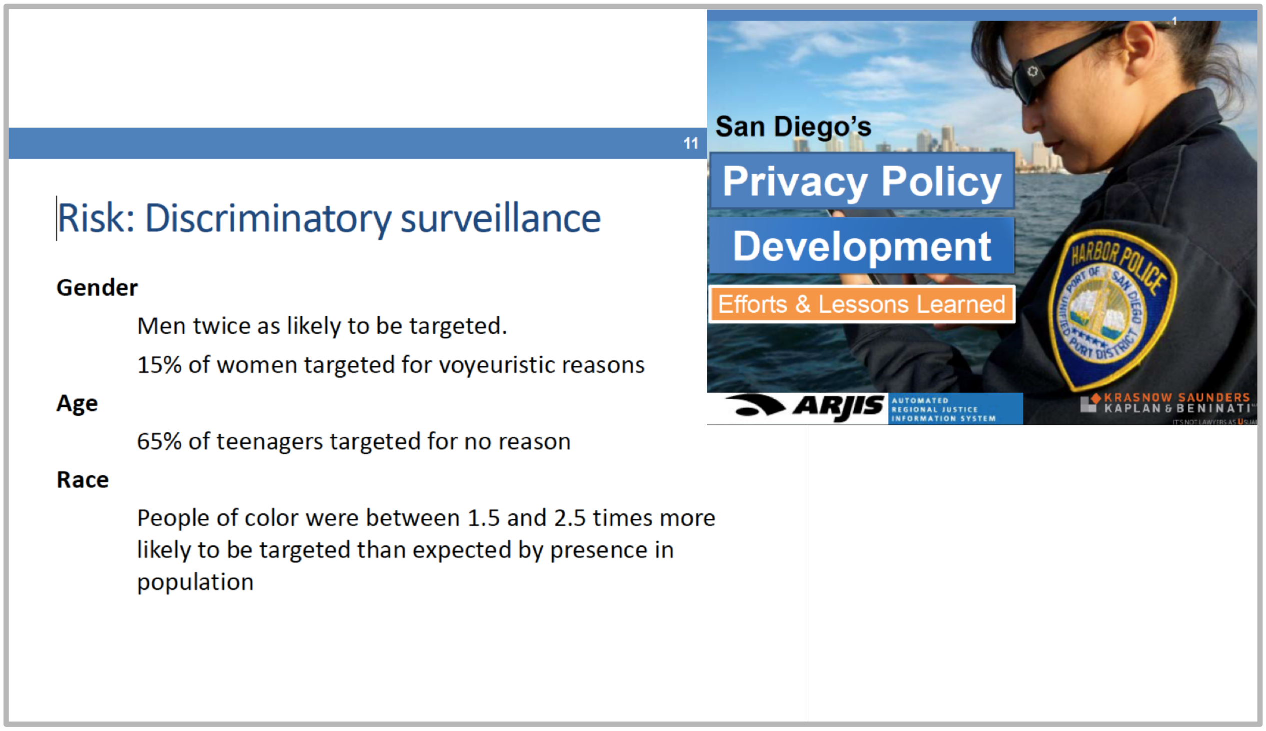
[20] *See* discussion *infra* Section I.D. of how face recognition technology is misused.

[21] *See* Jeremy C. Fox, *Brown University Student Mistakenly Identified as Sri Lanka Bombing Suspect*, Boston Globe, Apr, 28, 2019, https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html.

[22] *Id.*

context could result in an individual being wrongfully arrested, accused of, or even convicted of a crime.

Disparate impact on communities of color. Of even greater concern, mistakes made by imperfect face recognition systems will be borne disproportionately by communities of color. Communities of color disproportionately are the targets of police surveillance, face recognition being no exception to this rule. For example, in San Diego, police used face recognition up to 2.5 times more on African American people than on anyone else.[23] People of color also are disproportionately enrolled in police face recognition databases. This is because the majority of police face recognition systems across the country rely on mugshot databases to make identifications, and because African-Americans are statistically more likely than other demographic groups to be arrested by law enforcement for the same crimes, mugshot databases contain photographs of African-Americans at a disproportionately high rate.



11

Risk: Discriminatory surveillance

Gender

Men twice as likely to be targeted.

15% of women targeted for voyeuristic reasons

Age

65% of teenagers targeted for no reason

Race

People of color were between 1.5 and 2.5 times more likely to be targeted than expected by presence in population

San Diego's

Privacy Policy

Development

Efforts & Lessons Learned

HARBOR POLICE
PORT OF SAN DIEGO
UNIFIED PORT DISTRICT
ARJIS
AUTOMATED REGIONAL JUSTICE INFORMATION SYSTEM
KRASNOW SAUNDERS KAPLAN & BENINATI

Image 1: A slide from a San Diego Association of Governments' presentation about regional police use of automated license plate readers and face recognition acknowledges that people of color are disproportionately targeted by surveillance technologies.

[23] Automated Regional Justice Information System, *San Diego's Privacy Policy Development: Efforts & Lessons Learned*, 11, *available at* https://drive.google.com/file/d/1ZR2jjiLcBMUKnHTRk1ZC248NbFUqNRww/view?usp=sharing.

In addition, automated facial analysis technologies—including face recognition technology—commonly exhibit demographic bias. These tools tend to make mistakes disproportionately on faces of women, young and old people, and people of color. To the extent that mistakes lead to misidentifications, this means that women, young and old people, and people of color will be misidentified by automated face recognition tools at higher rates than other people.

There is a large body of research on demographic bias in automated facial analysis algorithms. In 2012, a team of scientists—including the FBI's own technologist—studied three commercially available face recognition algorithms and found that all three algorithms performed significantly worse on faces of women than on faces of men, on faces of African Americans than on faces of other races, and on faces in the age range 18 to 30 than on older faces.[24] A few years later, as I and my colleagues were researching law enforcement use of face recognition technology, we interviewed representatives of two leading face recognition vendors for law enforcement regarding potential bias challenges and found that "engineers at neither company could point to tests that explicitly checked for racial bias."[25]

Just last year, two computer scientists studying a different kind of automated facial analysis algorithm—gender classification algorithms, which attempt to determine the gender of an evaluated face—also encountered demographic bias. Joy Buolamwini and Timnit Gebru reported that three commercially available gender classification algorithms all produced the highest error rates (20.8%–34.7%) when analyzing the faces of women with darker skin.[26] Not only did Buolamwini and Gebru find these biased performance problems, but they also reported that at the time of their study, the most commonly available datasets used for testing performance of automated facial analysis algorithms all failed to adequately represent darker-skinned faces, and especially darker-skinned women.[27] As a result, typical performance tests of

[24] Brendan F. Klare, Mark J. Burge, Joshua C. Klontz, Richard W. Vorder Bruegge, & Anil K. Jain, *Face Recognition Performance: Role of Demographic Information*, 7 IEEE Transactions on Info. Forensics & Sec. 1789 (2012).
[25] Garvie, Bedoya & Frankle, *The Perpetual Line-Up*.
[26] Joy Buolamwini & Timnit Gebru, *Gender Shades*, 81 Proceedings of Machine Learning Research 1, 11 (2018).
[27] *Id.*

facial analysis algorithms would be less likely to uncover certain bias problems, because they would not be able to thoroughly test for all biases.

Also last year, ACLU tested Amazon's face recognition product, "Rekognition," which the company markets to private actors and government agencies alike, and found that Rekognition's face identification tool falsely matched the faces of people of color with photos in a mugshot database at a disproportionately high rate.[28] Also in 2018, results were released of face recognition tests that took place as part of a 2018 Department of Homeland Security evaluation, and showed that efficiency and accuracy were both affected by demographics, including skin tone.[29]

D. Face recognition is misused and shrouded in secrecy.

When we examine the use of face recognition by law enforcement, we cannot ignore that it operates within our broader criminal justice system, and that its primary goal is to identify people to be arrested. In the absence of regulation the way the technology is currently used by police contains serious risks of misidentification. In the absence of transparency, these uses threaten to violate the due process rights of those arrested.

Face recognition misuse. The problems stemming from technical shortcomings of face recognition—including widespread algorithmic bias—would be concerning even if the technology were used responsibly by those

[28] Jacob Snow, ACLU, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, July 26, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.
[29] Cynthia M. Cook, John J. Howard, Yevgeniy B. Sirotin, Jerry L. Tipton, & Arun R. Vemury, *Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems*, IEEE Transactions on Biometrics, Behavior, and Identity Science at 8 (2019)("[M]odeling showed that mated similarity scores were higher for men versus women, for older versus younger people, for those without eyewear, and those with relatively lighter skin. Of the different demographic covariates examined, our calculated measure of skin reflectance had the greatest net effect on average biometric performance."). A Florida Institute of Technology study found similar differential error rates, holding that "[f]or a desired FMR [false match rate, or misidentification rate], the threshold setting would need to be different for each demographic group." Michael King, *Demographic Effects of Race on Face Recognition*, IFPC 2018, 11 (Nov. 27, 2018), *presentation available at* https://nigos.nist.gov/ifpc2018/presentations/15_king_18-11-27_DemographicEffectsFaceRecognitionNIST_Update.pdf.

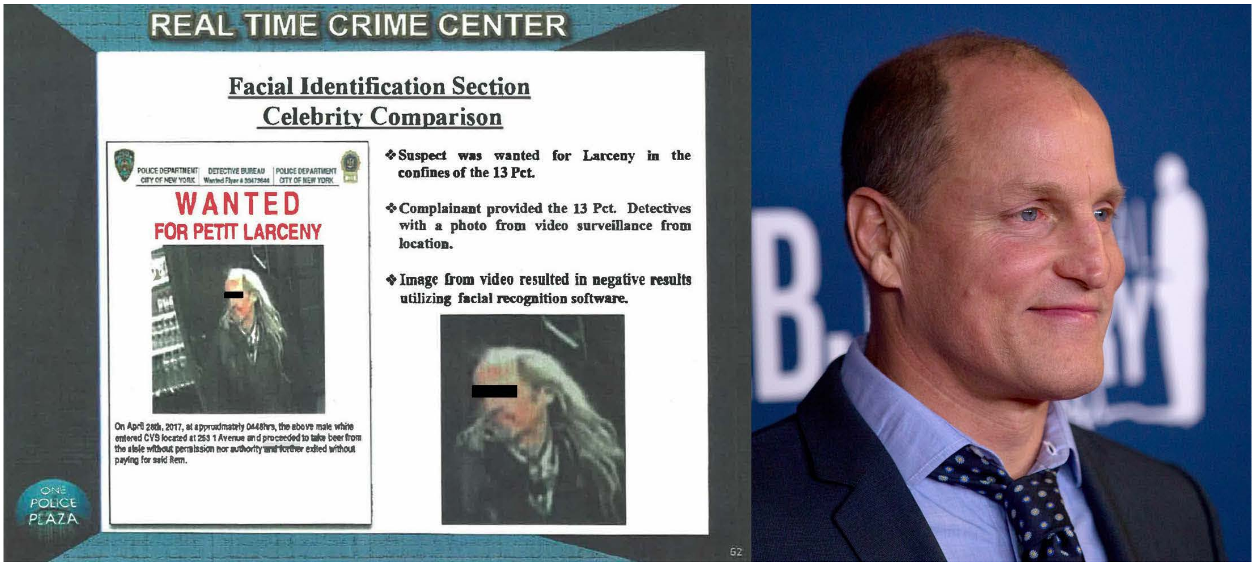
with access to it. But public records from agencies around the country indicate that this is not the case. As explained in depth in a report the Center on Privacy & Technology published last week, my research has found that law enforcement agencies routinely misuse this technology, expecting to receive viable investigative leads from fundamentally unreliable, incomplete, heavily edited, or wrong evidence.[30]

Numerous law enforcement agencies regularly fabricate, in whole or in part, the photographs of suspects prior to submitting those photographs to search by a face recognition system. When agencies have a photograph of an suspect that is blurry, of low quality, or partially obscured, they simply make up the missing evidence so that they can make use of their face recognition system. Some examples of this from my research:

- The New York Police Department (NYPD) has used "celebrity comparisons" to find suspects whose photographs are too poor quality to return face recognition results. This practice consists of identifying a celebrity or other person that detectives think the suspect looks like, then submitting that other person's biometric face template to the face recognition system to find the suspect. The NYPD has done this on at least two occasions: using a photograph of Woody Harrelson to find a suspect wanted for petit larceny of a few beers; and using a photograph of the basketball player J.R. Smith to find someone suspected of assault in Brooklyn.[31]

[30] Garvie, *Garbage In, Garbage Out*.

[31] *Id.*



REAL TIME CRIME CENTER

Facial Identification Section

Celebrity Comparison

POLICE DEPARTMENT CITY OF NEW YORK | DETECTIVE BUREAU Wanted Flyer # 33473644 | POLICE DEPARTMENT CITY OF NEW YORK

WANTED

FOR PETIT LARCENY

[redacted]

On April 28th, 2017, at approximately 0448hrs, the above male white entered CVS located at 253 1 Avenue and proceeded to take beer from the aisle without permission nor authority and further exited without paying for said item.

- ❖ Suspect was wanted for Larceny in the confines of the 13 Pct.
- ❖ Complainant provided the 13 Pct. Detectives with a photo from video surveillance from location.
- ❖ Image from video resulted in negative results utilizing facial recognition software.

[redacted]

Image 2: On multiple occasions, NYPD submitted the photo of a suspect's celebrity doppelgänger to its face recognition system when the suspect's own photo failed to return useful matches.

- The NYPD also uses Photoshop and other photo editing tools to edit or add in new features into suspect photographs. These practices include: cutting and pasting open eyes from a photograph of another person over the closed eyes of the suspect; cutting and pasting a closed mouth from another person's photograph over the open mouth of the suspect; combining two face photographs of two different people to attempt to identify one of those people; using the "blur effect" tool to add pixels to a photograph that was otherwise of too low quality to generate face recognition results; and changing the pose of a face using 3D modeling.[32]

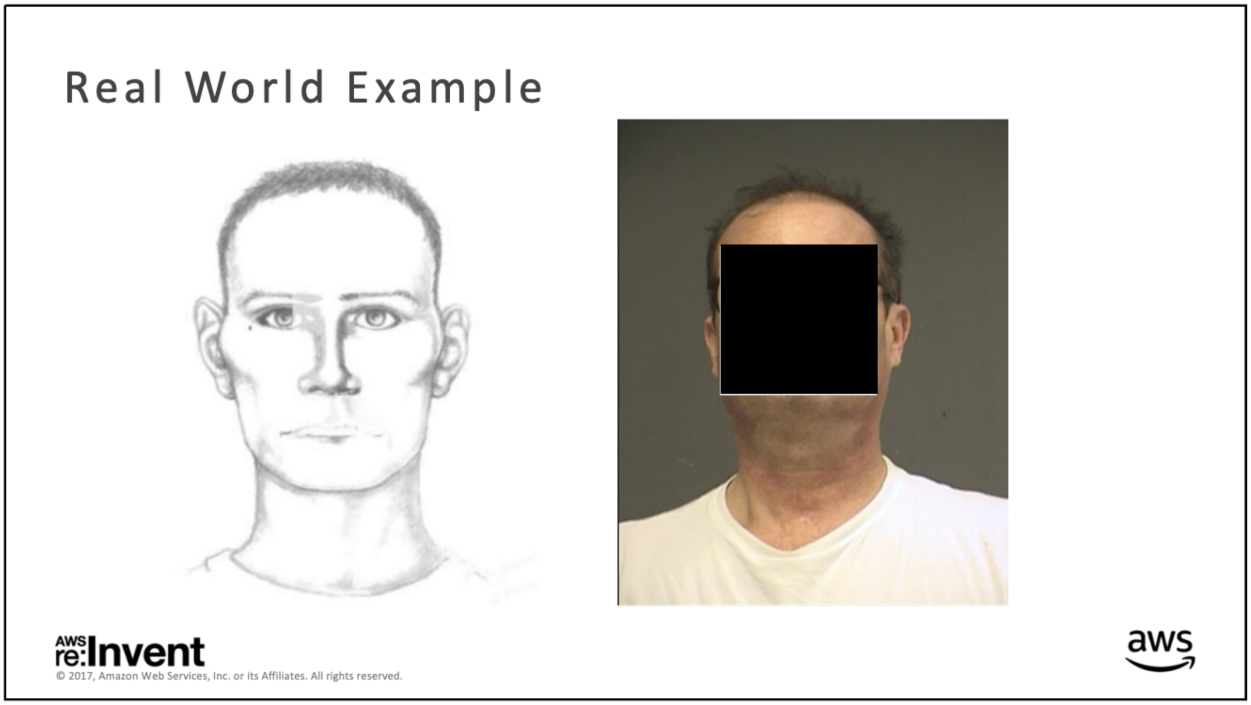
  Photo editing techniques are likely used by other agencies as well. DataWorks Plus, the face recognition vendor company for the NYPD and a number of other agencies—including the Michigan and Virginia State Police, the Chicago and Detroit Police Departments, the Los Angeles County Sheriff, and others[33]—comes with an "image manipulate screen" and other toolbars that have many of these editing tools built in.[34]

[32] *Id.*

[33] *See* Garvie, Bedoya & Frankle, *The Perpetual Line-Up*; Garvie, *Garbage In, Garbage Out.*

[34] Dataworks Plus, *FACE Plus Case Management User Guide*, 13–14 (date unknown), *available at*

- At least six police departments across the country permit or encourage the use of face recognition on forensic sketches—hand drawn or computer generated representations of faces based on the description offered by an eyewitness.[35] Studies that have evaluated the performance of face recognition systems on forensic sketches have concluded that this practice will fail to produce reliable results. One study found that only in 5% of searches on sketches, the right match was returned in the top 200 possible matches. In the remaining 95% of searches, the right match wasn't returned at all.[36]



Real World Example

[redacted]

AWS re:Invent
aws

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Image 3: At least six police departments across the country permit or encourage the use of face recognition on forensic sketches – a practice studies conclude will have a very high failure rate.

Over reliance on face recognition results. Many agencies state that no one is arrested solely on the basis of a face recognition match, and that additional investigative steps are conducted after the face recognition search and prior

https://drive.google.com/file/d/1f2S9FRq2HsR4AG8Vzuwsj7iPFEAnVHq3/view?usp=sharing.

[35] Garvie, *Garbage In, Garbage Out.*

[36] Scott Klum, Hu Han, Anil Jain, & Brendan Klare, *Sketch Based Face Recognition: Forensic vs. Composite Sketches* (2013), *available at* https://openbiometrics.org/publications/klum2013sketch.pdf.

to an arrest being made.[37] In theory, this would mean that officers must corroborate the identification made by the face recognition system through other, independent investigation, a valuable check against possible misidentification.

In reality, my research has found that this is not always the case. Agencies in multiple jurisdictions have relied almost exclusively on the results of a face recognition system to identify someone for arrest, greatly increasing the risk of misidentification. As published in the Center on Privacy & Technology's recent report: *Garbage In, Garbage Out*:

- In a recent case, NYPD officers apprehended a suspect and placed him in a lineup solely on the basis of a face recognition search result. The ultimate arrest was made on the basis of the resulting witness identification, but the suspect was only in the lineup because of the face recognition process.

- NYPD officers made an arrest after texting a witness a single face recognition "possible match" photograph with accompanying text: "Is this the guy…?" The witness' affirmative response to viewing the single photo and accompanying text, with no live lineup or photo array ever conducted, was the only confirmation of the possible match prior to officers making an arrest.

- Sheriffs in Jacksonville, Florida, who were part of an an undercover drug sale arrested a suspect on the basis of the face recognition search. The only corroboration was the officers' review of the photograph, presented as the "most likely" possible match from the face recognition system.

[37] For example, the NYPD's Chief of Detectives Memo on face recognition states: "Real Time Crime Center Facial Identification Section (FIS) analyst determines that Subject is POSSIBLY the suspect whose image is depicted in the video and / or photograph regarding a crime. A FIS Possible Match does NOT constitute a positive identification and does NOT establish probable cause to arrest the Subject. Additional investigative steps MUST be performed in order to establish probable cause to arrest the Subject." (emphasis and capitalization in original). *Real Time Crime Center Facial Identification Section (FIS) Notification, Chief of Detectives Memo No. 3* (Mar. 27, 2012), *available at* https://drive.google.com/file/d/1M5kUIu3GYeeL_3Ah2fpmhAwgg8dY7WpG/view?usp=sharing.

- A Metro Police Department officer in Washington, D.C., similarly printed out a "possible match" photograph from MPD's face recognition system and presented that single photograph to a witness for confirmation. The resulting arrest warrant application for the person in the photograph used the face recognition match, the witness confirmation, and a social media post about a possible birth date (month and day only) as the only sources of identification evidence.[38]

No transparency to defendants or the courts. The threat of misidentification by a face recognition system would also be mitigated if defendants were told if and how it was used to identify them. But they're not. Surveys of public defenders in numerous jurisdictions around the country have revealed a consistent failure on the part of the prosecution to disclose information relating to face recognition searches.[39]

This is more than an oversight. The 1963 Supreme Court case *Brady v. Maryland* held that the suppression of evidence that is material to the guilt or innocence of the accused violates his due process rights under the Fourteenth Amendment.[40] As conducted by law enforcement, face recognition searches produce such evidence.

As outlined above, the original photographic evidence may be of poor quality, and subject to being heavily edited prior to the search being run. In fact, the search may not be on the suspect's face at all, as in the case of a "celebrity comparison" search, or in part, as with a search where the someone else's eyes, mouth, or other facial feature was cut and pasted into the suspect's photograph. Or it may not be a photograph at all, and instead an artist's rendering of what a witness told him the suspect looked like. These practices directly call into question the reliability of the identification.

[38] Garvie, *Garbage In, Garbage Out.*
[39] *Id. See* Garvie, Bedoya & Frankle, *The Perpetual Line-Up* (describing how our earlier research found that in the 15 years the Pinellas County Sheriff's Office had been using face recognition technology, the Public Defender's Office for the region had never received information about the technology as part of *Brady* disclosure.) *See* Reply Brief of Appellant at 7, Willie Lynch v. State of Florida, No. 1D16-3290 (Fla. 1st DCA 2017) ("It was there [during depositions] that the defense found out that Tenah used a biometric facial recognition program to identify Appellant. Up until then the State had failed to disclose that information.").
[40] Brady v. Maryland, 373 U.S. 83, 87 (1963).

Moreover, face recognition searches typically produce a number of "possible match" candidates—something that people accused of crimes often are not told. The NYPD, for example, sets its face recognition system to produce 200 or more possible matches, subject to review by an analyst. Imagine a defendant, who is arrested and charged on the basis of the search, was ranked 150 out of 200 possible matches, something law enforcement agencies concede may happen.[41] Or, as described by the analyst responsible for Washington Country, Oregon's face recognition system: "We found in our testing that something that returned a 99% wasn't the person .... And some results that returned 73% were indeed that person."[42] In both of these examples, the face recognition algorithm concluded that at least one person—and as many as 149 people—looked *more* like the suspect than the person arrested and charged.[43] Yet the full candidate list—even if it contains 100 or more people considered by the algorithm to be more likely to be the suspect—is almost never seen by the defendant.

Real-world consequences. Earlier this year, the Center on Privacy & Technology joined the American Civil Liberties Union (ACLU), Electronic Frontier Foundation (EFF) and Innocence Project in filing an *amicus curiae* brief in the Florida Supreme Court.[44] This brief is in support of the Mr. Lynch, a man serving an eight year sentence after being identified by face recognition as the suspect in a $50 undercover drug sale. Mr. Lynch was not told by the prosecution that the Jacksonville Sheriff's Office identified him using face recognition. He was never allowed to view the four other "possible matches" that the face recognition system thought could also be the suspect.

[41] The NYPD has set its system to return 200 or more possible matches, because according to its analysts, the correct match may be that low in the algorithm's ranking of possible matches. *NYPD Real Time Crime Center Facial Identification Section (FIS) presentation by Detective Markiewicz* (Sept. 17, 2018) (notes on file with author).

[42] *See* On Point, *San Francisco Bans Facial Recognition Tech Over Surveillance Bias Concerns*, On Point (May 16, 2019), https://www.npr.org/podcasts/510053/on-point.

[43] It also means that the rank order of the candidate list may not reliably indicate who is more or less likely to be a match. As a consequence, the entire list should be turned over to the defense in all cases, regardless of the defendant's place in that rank order.

[44] *Amici Curiae* Brief of ACLU, ACLU of Florida, EFF, Georgetown Law's Center on Privacy & Technology, and Innocence Project in Support of Petitioner, No. SC2019-0298 (Fla. Sup. Ct. 2019), *available at* https://efactssc-public.flcourts.org/casedocuments/2019/298/2019-298_notice_86166_notice2dappendix2fattachment20to20notice.pdf.

Mr. Lynch is black, meaning that the algorithm may have performed less reliably on him because of his skin tone.[45]

The prosecution itself, in recognizing the issues with how Mr. Lynch was identified, acknowledged on the record that the face recognition system was probably not reliable enough to meet the evidentiary standards for use at trial.[46] Despite this, Mr. Lynch was convicted at the trial court level, and his conviction was affirmed on appeal. He maintains his innocence.

This case represents a failure on the part of the courts to uphold Mr. Lynch's constitutional right to due process. It represents just one of an unknown number of cases where face recognition was used, unbeknownst to the defense, using any number of unreliable techniques, untrained analysts, and insufficiently corroborated results. The stakes are too high in criminal investigations to rely on fundamentally unreliable face recognition searches, and to simultaneously obscure these methods from the defense.

2. Face recognition is advancing rapidly. Privacy law isn't catching up.

The conversation about how to deal with these concerns and problems cannot be delayed. Face recognition already is already more pervasive and advanced than most people realize, and we should only expect it to become more so. And at present, the law does little to nothing to protect against the myriad, serious concerns raised by police use of face recognition technology.

A. Face recognition is more pervasive and advanced than people realize.

It would be hard to overstate the rapid pace with which face recognition technology has been adopted by law enforcement agencies—federal, state, and local—across the country. Face recognition has become a routine law enforcement tool. In 2016, the Center on Privacy & Technology estimated *conservatively* that at least one quarter of the 18,000 law enforcement agencies across the country have access to a face recognition system.[47] This number represents what I could confirm based on records requests sent to

[45] *Id.* at 2–3.
[46] *Id.* at 8–9.
[47] Garvie, Bedoya & Frankle, *The Perpetual Line-Up*.

100 law enforcement agencies—imagine what the real total would be if we knew the capabilities of every agency.

Some of these systems, like the one operated by the FBI, are searched thousands of times per year.[48] The Pinellas County Sheriff's Office system is searched on average 8,000 times per *month* by more than 240 agencies that have direct access.[49] A detective working for the NYPD Facial Identification Section estimates that 8,000 criminal cases in 2018 alone will have used a face recognition search.[50]

Many of these systems run face recognition searches against millions of Americans. Over half of all American adults can be identified by police using face recognition—thanks to getting a driver's license in one of at least 31 states.[51] An additional 13 states have face recognition-enabled driver's license databases; we don't yet know the degree to which they share that information with law enforcement.[52]

Police face recognition is becoming more advanced, as well. It is tempting to think that face recognition as a real- or near real-time surveillance tool, with the serious risks its poses to our First and Fourth Amendment rights as described above, is an unlikely or remote future for the United States. But for millions of Americans, this is an imminent reality.

The Chicago Police Department (CPD) sought to implement a face surveillance system as early as 2009. The company providing the system describes the capability Chicago purchased as providing "real time screening using facial recognition on Chicago's vast camera monitoring system which includes nearly 20,000 street, transit and other video cameras located

[48] The Government Accountability Office found that the FBI conducted over 118,000 searches of its Next Generation Identification Interstate Photo System in a four-year period, and states requested 20,000 searches of the FBI database in the same time period. U.S. Gov't Accountability Office, GAO-16-267, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy,* 49, 12 (May 2016).
[49] Garvie, Bedoya & Frankle, *The Perpetual Line-Up*.
[50] Garvie, *Garbage In, Garbage Out*.
[51] *See supra* note 7 and accompanying text.
[52] This is information I have learned from research I have not yet published. I have the supporting documents and am happy to share and discuss them with Congress upon request.

throughout the city."[53] The system is designed to compare faces captured on video surveillance to chicago's database of around seven million mugshots.[54] While CPD maintains the system is not currently used, no rules exist governing its potential future use—the only face recognition policy provided by CPD states that "[p]olicies, training and protocols *will be* developed and maintained by the Bureau of Detectives."[55]

The Detroit Police Department (DPD) purchased the same system in 2017, designed to operate on "not less than 100 concurrent video feeds."[56] Those feeds are from cameras installed on gas stations and liquor stores, but also clinics, churches, schools, residential buildings, and other locations that have joined Detroit's Project Green Light public-private partnership.[57] DPD does have a policy, but it allows for the vast expansion of the department's face surveillance capabilities, stating that "DPD may connect the face recognition system to any interface that performs live video, including cameras, drone footage, and body-worn cameras."[58]

Chicago and Detroit are not alone in exploring the use of face surveillance technology. Pilot programs in Orlando, Florida, Washington, D.C., and New York City, New York are all exploring the potential of face recognition to

[53] Detroit Police Department *Professional Services Contract between City of Detroit, Michigan and DataWorks Plus, Contract No. 6000801* (July 31, 2017), *available at* https://drive.google.com/file/d/1IuvreaPV_8YStkNzT7RK5Z4Uyq4p6Btx/view?usp=sharing. For a more detailed description of the Chicago surveillance system and the concerns it raises, *see* Garvie & Moy, *America Under Watch*. *See also* DataWorks Plus, Company News, http://www.dataworksplus.com/newsarchives.html (stating that "The Chicago Transit Authority purchased a Facial Recognition System for Trains and Platforms to utilize Real Time Screening on the Transit System. The system uses the Chicago Police Departments mugshot database comprised of over 3 million records with a real time database update feed.").

[54] *Id.*

[55] Chicago Police Dep't, *Notice D13-11: Facial Recognition Technology* (Aug. 23, 2013), *available at* https://drive.google.com/file/d/1f2S9FRq2HsR4AG8Vzuwsj7iPFEAnVHq3/view?usp=sharing.

[56] *Id.*

[57] *See* Garvie & Moy, *America Under Watch*.

[58] DPD, *Crime Intelligence Unit Standard Operating Procedure for Face Recognition* (July 1, 2018, revised April 1, 2019) (emphasis added), *available at* https://drive.google.com/file/d/1mNZ5lCobLNPiuaTR78MT0UeMJ6dwjJbg/view?usp=sharing.

identify people in real-time, remotely and in secret, from video feeds that keep a constant eye on these cities' streets.[59]

B. The law does little to nothing to protect against all of these problems.

Although this technology—despite its many flaws—is spreading extremely fast, the law does little to nothing to protect against the many problems detailed above. Other than a recently-adopted ban in San Francisco, there is no comprehensive local, state, or federal law addressing face recognition technology, setting legal or technical standards for the technology, or even forcing transparency as it relates to use of this and related tools. All we have are tidbits in various laws: Oregon and New Hampshire prohibit face recognition on police body cameras;[60] Maine and Vermont restrict police face recognition use in conjunction with drone footage;[61] a handful of states restrict police access to search driver's license face recognition systems.[62]

But for the vast majority of police face recognition applications in the vast majority of jurisdictions, the law is silent.

As discussed above, face recognition technology poses risks that the First, Fourth, and Fourteenth Amendments may—and should—protect against. But there is no case law yet that unequivocally extends these constitutional protections to the technology. It may be a long time before the Supreme Court addresses these questions directly. And in the meantime, we can only expect the technology to become more widespread and more advanced.

3. We need to hit the pause button on face recognition.

In 2016, I co-authored a landmark report on police use of face recognition technology in the United States. The report recommended that Congress and state legislatures adopt common sense legislation to comprehensively regulate law enforcement face recognition.[63]

[59] *See* Garvie & Moy, *America Under Watch.*
[60] Or. Rev. Stat. § 133.741(1)(b)(D); N.H. Rev. Stat. Ann. § 105-D:2(XII).
[61] Vt. Stat. Ann. tit. 20 § 4622(d)(2); Me. Rev. Stat. Ann. tit. 25 § 4501(5)(D)
[62] Me. Rev. Stat. Ann. tit. 29-A, § 1401; Mo. Ann. Stat. § 302.189; N.H. Rev. Stat. Ann. § 260:10-b and N.H. Rev. Stat. Ann. § 263:40-b; Vt. Stat. Ann. tit. 23, § 634(c).
[63] Garvie, Bedoya, & Frankle, *The Perpetual Line-Up* at 62 (detailing recommendations); 102 (offering model face recognition legislation).

Since then, a dramatic range of abuse and bias has surfaced. Baltimore County Police used the technology to identify and arrest people protesting the death of Freddie Gray. A Brown University student was falsely identified as a possible terrorist suspect responsible for attacks in Sri Lanka. Research by Joy Buolamwini, Timnit Gebru, and the ACLU of Northern California verified that the technology still exhibits race and gender bias in its accuracy rates.

I now believe that federal, state, and local governments should place a moratorium on police use of face recognition. Communities need time to consider whether they want face recognition in their streets and neighborhoods.

Jurisdictions that move to ban the technology outright are amply justified to do so. The power that this technology gives to law enforcement, combined with the secrecy with which the technology has been deployed, its persistent inaccuracy and race and gender bias, and the way it has been misused and abused, make face recognition an existential threat to fundamental freedoms in our society. A city's residents do not need to wait until a person's life is upended by a face recognition misidentification to decide that this technology is dangerous and unwelcome in their community.

For jurisdictions that do want to allow certain uses of face recognition, I recommend a highly restrictive combination of bans; regulation; and court, public, and expert oversight:

- **Certain uses of the technology should be banned outright.** In 2018, the CEO of Axon, the largest U.S. manufacturer of police body cameras, openly considered adding a real-time face surveillance capacity to its products, a move that would let police body cameras quietly scan the face of every man, woman, and child that passes in front of an officer.[64] This proposal is dangerous. It risks sending erroneous face recognition alerts to armed officers in the field, particularly when an officer walks past someone hailing from a demographic group on which the technology is proven to underperform. For these reasons, face

[64] Scott Simon, *Body Camera Maker Weighs Adding Facial Recognition Technology*, National Public Radio's Weekend Edition (May 12, 2018), https://www.npr.org/2018/05/12/610632088/what-artificial-intelligence-can-do-for-local-cops.

surveillance on body cameras, drones, and dashcams should be prohibited.[65] The technology should never be used to monitor any First Amendment-protected activities. Any meaningful regulation of face recognition must include certain outright bans on uses that are too susceptible to abuse or misuse.

- **Face surveillance should be banned or severely restricted.** In investigative or forensic face identification, a specific, targeted individual's face is sought to be identified. In face surveillance, every face appearing in archival or real-time footage is scanned and compared against a watchlist.[66] This form of dragnet face recognition turns the spirit of the Fourth Amendment on its head; it treats every person as a criminal suspect. It also threatens to erase the ability of a person to be just a "face in the crowd," or to participate in anonymous, First Amendment-protected speech. Already, protesters report having to obscure their faces for the precise purpose of engaging in peaceful, anonymous protest.[67] Multiple reports suggest that the Chinese government tracks the movements of Uighurs, members of a Chinese Muslim minority, through a vast face surveillance system.[68]

[65] In 2018 my organization publicly adopted this position in a coalition letter we wrote to the new "AI Ethics Board" of Axon, a major vendor of police body-worn cameras. The letter, signed by 42 civil rights, racial justice, and community organizations, argued that integration of real-time face recognition with body-worn camera systems would be "categorically unethical." *Letter to Axon AI Ethics Board regarding Ethical Product Development and Law Enforcement*, The Leadership Conference on Civil & Human Rights (Apr. 26, 2018), *available at* https://civilrights.org/resource/axon-product-development-law-enforcement/.

[66] "Face surveillance" is often referred to as "real-time face recognition" although it need not be conducted in real-time to pose a threat to privacy, civil rights, and civil liberties. For a taxonomy of uses and risks of face recognition, see Section IV of our 2016 report, *The Perpetual Line-Up*. Garvie, Bedoya & Frankle, *The Perpetual Line-Up* at 16–20 ("A Risk Framework for Law Enforcement Face Recognition").

[67] Craig Timberg, *Racial profiling by a computer? Police facial-ID tech raises civil rights concerns.* The Washington Post (Oct. 18, 2016) (quoting a protester who covers their face to avoid face recognition).

[68] *See, e.g.*, *China Uses Facial Recognition to Fence In Villagers*, Bloomberg (Jan. 17, 2018), https://www.bloomberg.com/news/articles/2018-01-17/china-said-to-test-facial-recognition-fence-in-muslim-heavy-area ("The Muslim-dominated villages on China's western frontier are testing facial-recognition systems that alert authorities when targeted people venture more than 300 meters (1,000 feet) beyond designated "safe areas," according to a person familiar with the project. The areas comprise individuals' homes and workplaces…").

Any lawmaking body, from a city council to the Congress, would be plainly justified in banning this form of surveillance. Jurisdictions that opt to allow it should reserve it for public emergencies threatening human life, where all other measures have failed. Even then, use of the technology should require sign-off from a senior executive branch official, like the governor of a state, and then a further approval by a court, which should place strict rules on how and when the technology is used, whom it is used to locate or identify, and how the public will be notified of the surveillance.

- **Searches of DMV photos should be banned or severely restricted.** As explained above and in our 2016 report, never before—not with DNA or fingerprints—have most American adults been enrolled in a de facto criminal biometric database. It is shocking that this mass enrollment has occurred largely in secret and despite the repeated rejection of public proposals to create a national ID. In fact, of the 31 states that currently allow police or FBI face recognition searches of DMV photos, it appears that only two actually have state statutes that expressly allow the use of face recognition on driver's license photos.[69]

  These types of searches should be allowed only after it is unambiguously and affirmatively permitted by state law. Likewise, the federal government should not conduct face recognition searches of DMV photo repositories unless state law expressly and unambiguously allows those searches.

- **Face recognition searches should be restricted to serious, violent offenses.** In 2016, I suggested that face recognition searches be allowed for felonies (in the case of mugshot searches) or serious offenses identified in the Wiretap Act (for searches of driver's license photos). Earlier this year, I joined several law enforcement professionals in calling for a heightened standard, one that restricted face recognition searches to Uniform Crime Reporting Part I offenses (e.g., criminal

[69] A state law survey by the Center on Privacy & Technology has identified only Florida and Texas as having statutes expressly and unambiguously allowing law enforcement to use face recognition on DMV photos for criminal investigations beyond identity fraud. Fla. Stat. Ann. § 943.05; Tex. Code Ann. § 521.059.

homicide, forcible rape, robbery) as well as kidnapping and child exploitation.[70] In light of what we know about misuse and abuse of this technology, as well as its susceptibility to bias, this list should be further narrowed to exclude property crimes (e.g., larceny) that are non-violent and pose no threat to physical safety.

- **Institute mandatory and public accuracy and bias testing in operational conditions.** Should a jurisdiction choose to enable police face recognition use, that system must be subject to independent testing for accuracy across demographic groups and under operational conditions. Testing must take into account all demographics that may affect the performance of the system, alone and in combination. It must also contemplate how law enforcement agencies use the technology, including on low-quality or edited images, if that remains a permitted practice. Results of these accuracy tests should be easily accessible both to the public at large and to criminal defendants.

- **Institute mandatory notice to defendants and annual reports to the general public.** When criminal suspects are wiretapped, they are eventually notified of that fact.[71] What's more, any member of the public can go online and review a public report, compiled by the Administrative Office of the U.S. Courts, that tells them—by specific jurisdiction—how often wiretaps were authorized, what crimes they were authorized to investigate, and whether or not people were arrested or convicted for those crimes.[72] This is because the Wiretap Act requires this minute level of transparency.[73] These notice requirements and reports are integral instruments of legal and democratic accountability.

[70] *See* The Constitution Project's Task Force on Facial Recognition Surveillance & Jake Laperruque, *Facing the Future of Surveillance*, The Project on Government Oversight (March 4, 2019) at IV (Recommendations) https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/#heading-14. *See also* Federal Bureau of Investigation, *Uniform Crime Reporting Handbook*, U.S. Dep't of Justice (2004) at 8 (listing Part 1 offenses) https://ucr.fbi.gov/additional-ucr-publications/ucr_handbook.pdf.

[71] 18 U.S.C. § 2518(8)(d) (requiring notice within 90 days to the subjects of wiretaps).

[72] *See, e.g.*, Administrative Office of the U.S. Courts, *2017 Wiretap Report* (Dec. 31, 2017) https://www.uscourts.gov/statistics-reports/wiretap-report-2017.

[73] 18 U.S. Code § 2519 (Reports concerning intercepted wire, oral, or electronic communications).

Any use of face recognition should be subject to similar notice and reporting requirements. In particular, jurisdictions should be required to report both convictions stemming from a face recognition-supported identification and any instance in which a person is wrongly investigated or arrested as a result of a misidentification.

- **Congress should respect local and state restrictions on face recognition.** As was shown in San Francisco, local and state legislatures are most likely to be the first to enact bans, moratoria, or other meaningful restrictions on face recognition. Congress and the federal government should respect those limits. Congress should prohibit federal law enforcement from using face recognition in a jurisdiction in a manner or form that has been prohibited by the voters or elected officials in that city or state. If Congress does not enact such a restriction, federal law enforcement should adopt it on their own. The members of the San Francisco City Council did not ban face recognition from their neighborhoods only to allow the FBI to do what its own law enforcement officers could not.

This is only a sampling of the limits I believe should apply to law enforcement's use of this technology. I would welcome the opportunity to work with members of Congress and this Committee, as well as local and state legislators, who wish to enact these and other restrictions.

4. Conclusion

I am grateful for the Committee's attention to these important issues, and for the opportunity to present this testimony. I look forward to your questions.