

Cummings U.C.  
5-22-19



House Committee on Oversight and Reform  
2157 Rayburn House Office Building  
Washington, DC 20515

May 17, 2019

Dear Chairman Cummings, Ranking Member Jordan, and Members of the Committee:

Thank you for your leadership in conducting this hearing to address the issue of facial recognition surveillance. We believe it is critical to establish proper checks and limits on this surveillance technology in order to protect constitutional principles, civil rights, and civil liberties. Enclosed for your consideration is The Constitution Project at the Project on Government Oversight's task force report on facial recognition surveillance. 8/9

Our report was written by stakeholders with a range of perspectives and expertise on the topic, including civil rights and civil liberties advocates, academics, technology experts, and law enforcement officials. We propose practical policy solutions Congress should enact now to address the growing threat of unrestricted facial recognition, including requiring warrants for using targeted facial recognition, limiting its use to a select set of serious crimes, and establishing rigorous testing and accuracy standards.

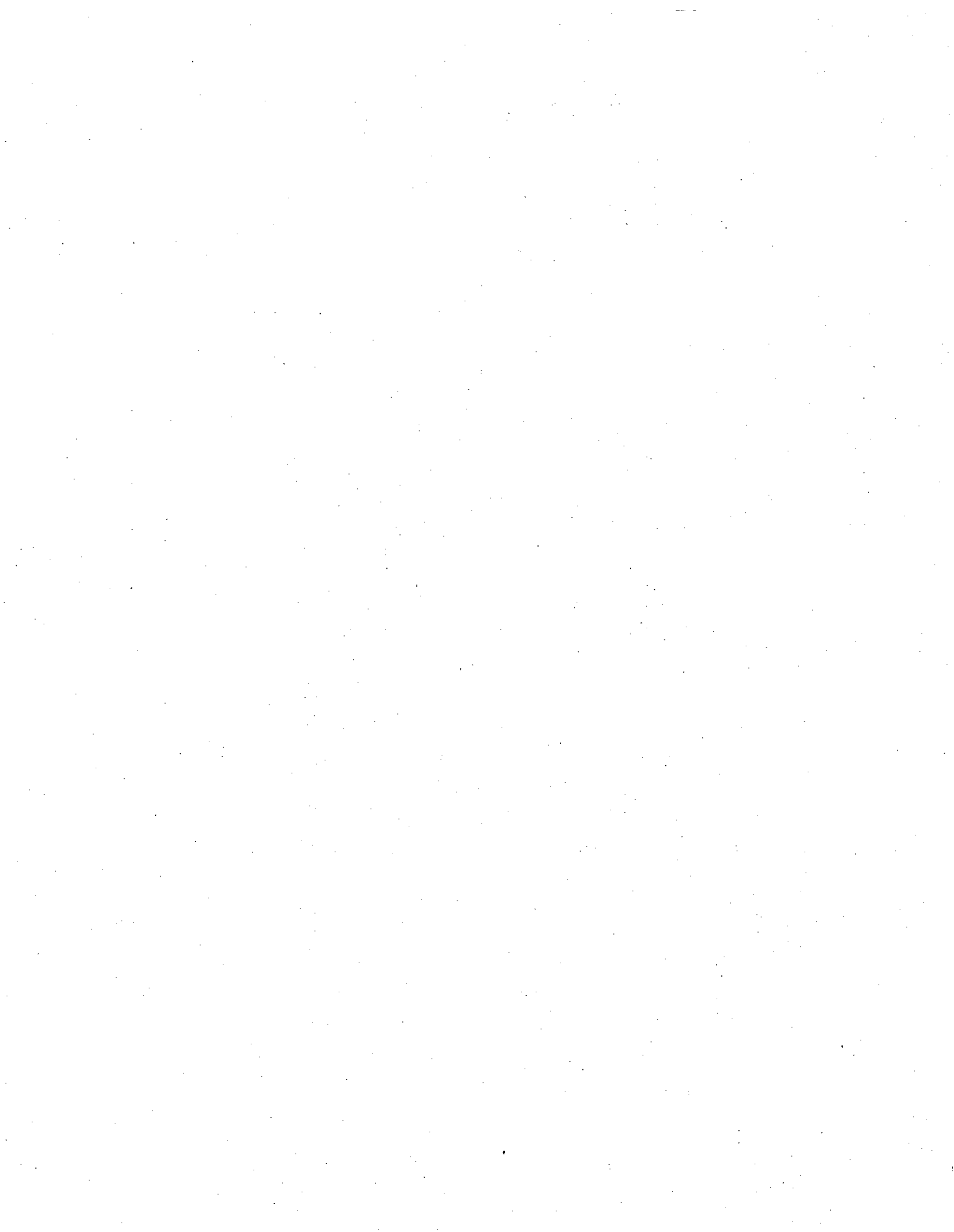
Our report analyzes a broad set of values put at risk by facial recognition surveillance. Privacy is the most vulnerable; it also endangers First Amendment activities, civil rights, and due process. The technology poses unprecedented risk of abuse and selective targeting based on race, religion, or political beliefs. Our report details instances in which this has already occurred. Given the risk of the technology misidentifying people, it could harm public safety and undermine police-community relations.

We believe it is crucial that Congress act swiftly to limit this already pervasive form of surveillance. At least one in four state or local police departments possesses the ability to run facial recognition searches either directly or via a partnering agency. The FBI ran over 52,000 facial recognition searches in fiscal year 2018, an average of over 4,000 searches per month


We applaud the Committee for its continued focus on this important issue. We hope the enclosed report and our other work on the topic aid the Committee in its work, and we are eager to provide any additional assistance we can in developing effective limits on facial recognition surveillance.

Thank you,

Jake Laperruque  
Senior Counsel  
The Constitution Project at POGO



# REPORT



## FACIAL RECOGNITION Facing the Future of Surveillance

March 4, 2019

TASK FORCE ON  
FACIAL RECOGNITION SURVEILLANCE

*Assembled by The Constitution Project at POGO*

**POGO**

## ABOUT

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.

We champion reforms to achieve a more effective, ethical, and accountable federal government that safeguards constitutional principles.

## ACKNOWLEDGEMENTS

### PRINCIPAL DRAFTER

Jake Laperruque

### CONTRIBUTORS

David Janovsky  
Sarah Turberville

### SPECIAL THANKS

Danni Downing  
Leslie Garvey  
Jennifer Lynch  
CJ Ostrosky  
Laurie Robinson  
Mia Steinle  
Daniel Van Schooten



PROJECT ON GOVERNMENT OVERSIGHT

1100 G Street NW, Suite 500

Washington, DC 20005

**WWW.POGO.ORG**

# Task Force Members

**Alvaro Bedoya** is the founding Executive Director of the Center on Privacy & Technology at Georgetown Law.

**David Brody** is Counsel & Senior Fellow for Privacy and Technology at the Lawyers' Committee for Civil Rights Under Law. He focuses on issues related to the intersection of technology and racial discrimination, equal opportunity, consumer privacy, free speech, hate group activity, and government surveillance.

**Kami Chavis** is a Professor of Law and Director of the Criminal Justice Program at Wake Forest University and a Former Assistant United States Attorney for the District of Columbia.

**Major Neill Franklin (Ret.)** is the Executive Director of the Law Enforcement Action Partnership and a 34-year veteran of the Maryland State Police and the Baltimore Police Department.

**Clare Garvie** is a Senior Associate at the Center on Privacy & Technology at Georgetown Law.

**Kelly Gates** is Associate Professor in Communication and Science Studies at the University of California San Diego.

**Chief Thomas J. Nestel, III** is a fourth-generation police officer who has served in a variety of law enforcement positions since 1982. He presently serves as the Chief of Transit Police for the Southeastern Pennsylvania Transportation Authority. Prior to accepting that position, he served as Chief of Police for Upper Merion Township (Montgomery County, PA) and as a Staff Inspector with the Philadelphia Police Department.

**James Trainum** is a Consultant for Criminal Case Review & Consulting, and was a Detective with the Washington, DC, Metropolitan Police Department from 1983 to 2010.

**Jeffrey L. Vagle** is an Affiliate Scholar at the Stanford Law School Center for Internet and Society, and was a Lecturer in Law and the Executive Director at the Center for Technology, Innovation and Competition at the University of Pennsylvania Law School.

**Kimberly Wehle** is a Professor of Law at the University of Baltimore School of Law and author of the forthcoming book, *How to Read the Constitution—and Why* (Harper Collins June 2019).

*Affiliations for identification purposes only.*

# Table of Contents

|   |           |
|---|-----------|
| Foreword .....  | 6         |
| <b>I. Introduction .....</b>  | <b>9</b>  |
| <b>II. Power and Use of Facial Recognition .....</b>                | <b>10</b> |
| Defining Facial Recognition .....                                   | 10        |
| How Facial Recognition Is Used .....                                | 11        |
| Development of Facial Recognition .....                             | 11        |
| Key Factors .....   | 12        |
| <i>Software</i> .....   | 12        |
| <i>Photo Databases</i> .....  | 13        |
| <i>Camera Sources</i> .....   | 14        |
| Closed-Circuit Television (CCTV) .....                              | 14        |
| Police Body Cameras .....   | 14        |
| Privately Owned Cameras .....                                       | 14        |
| Social Media Content .....  | 15        |
| <b>III. Constitutional Principles and Key Areas of Concern ....</b> | <b>16</b> |
| Privacy and Fourth Amendment Protections .....                      | 17        |
| <i>Privacy as a Vital Constitutional Principle</i> .....            | 17        |
| <i>Cataloging Sensitive Activities</i> .....                        | 18        |
| <i>Unchecked Location Tracking</i> .....                            | 19        |
| Prevalence of Misidentification .....                               | 20        |
| <i>Facial Recognition Can Be Highly Inaccurate</i> .....            | 20        |
| <i>Misidentification Creates Public Safety Risks</i> .....          | 21        |
| <i>Accuracy Problems Are Likely to Persist</i> .....                | 23        |
| Equal Protection and Civil Rights .....                             | 23        |

|  |           |
|--|-----------|
| Freedom of Expression and Association .....  | 25        |
| <i>Facial Recognition Endangers Anonymity and Obscurity</i> .....                        | 25        |
| <i>Facial Recognition Endangers First Amendment Activities</i> .....                     | 26        |
| <i>Facial Recognition Could Chill First Amendment Activities</i> .....                   | 26        |
| <i>Facial Recognition Endangers Press Freedoms</i> .....                                 | 27        |
| Due Process and Procedural Rights .....  | 28        |
| <i>Facial Recognition Could Undermine</i><br><i>Requirements for Police Action</i> ..... | 28        |
| <i>Facial Recognition Could Damage</i><br><i>Evidence and Defendants' Rights</i> .....   | 29        |
| Transparency and Accountability .....  | 30        |
| <b>IV. Recommendations</b> .....   | <b>31</b> |
| <b>Endnotes</b> .....  | <b>39</b> |

# Foreword

The revolution in digital technology has upended our society in many ways. Chief among these is that it has forced Americans to scramble to preserve the foundational balance of power between government and the people. For over two decades, The Constitution Project has sought to safeguard constitutional rights and principles when threatened by our government's national security and domestic policing practices. And our mission proves particularly salient—and challenging—in the digital age.

*Facing the Future of Surveillance* is our latest effort to formulate solutions to some of the most difficult constitutional questions of the day, through reports, amicus briefing, and advocacy. In 2017, we joined forces with the Project On Government Oversight (POGO) to amplify its role as the people's watchdog. Together, we have opened a new chapter in defending our democracy, including investigations and advocacy to protect individual rights in the face of excessive government surveillance.

Today, hundreds of millions of Americans' personal information is collected by private entities like cellular and internet service providers, as well as by public agencies like motor-vehicle departments. Anonymity in public is diminishing with the pervasive use of surveillance cameras. Local, state, and federal governments are amassing databases containing our fingerprints, DNA, retinal images, and photos of our faces on an unprecedented scale. New facial recognition technology could allow the government to use these databases to effortlessly determine the identity of everyone at a gathering or even throughout a city.

On the one hand, facial recognition can serve as a vital law enforcement tool to fight terrorism and crime. But the promise of this technology must be balanced with the imperative to protect constitutional rights and values, including privacy and anonymity, free speech and association, equal protection, and government accountability and transparency. And the government must be aware of the technical limits of even the most promising new technologies, and the risks of relying on computer systems that can be prone to error.

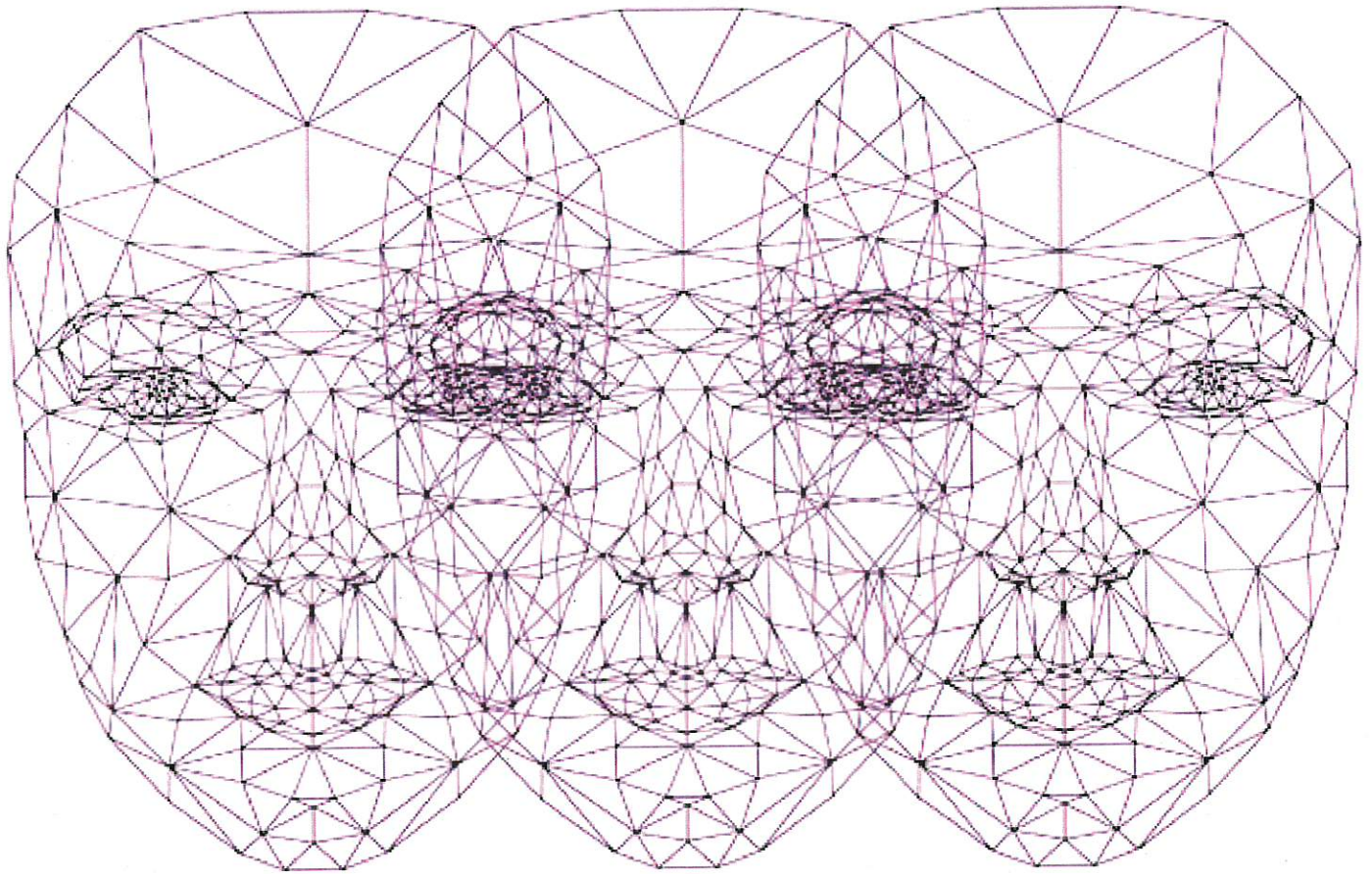
The law, however, has been slow to keep pace with the digital revolution and the perils it presents to fundamental rights and freedoms.



As facial recognition surveillance technology begins to make its way into the hands of police departments, we must now grapple with the prospect that the government could end anonymity with the push of a button. In China, the technology is already reshaping society into a high-tech version of George Orwell's Oceania, where millions of people are regularly cataloged for common activities. The United States, meanwhile, is at a tipping point: facial recognition is creeping into more and more law enforcement agencies with little notice or oversight, and there are practically no laws regulating this invasive surveillance technology. Meanwhile, ongoing technical limitations to the accuracy of facial recognition create serious problems like misidentification and public safety risks.

Recognizing the promise and risks presented by facial recognition, The Constitution Project at POGO convened a task force of experts and stakeholders from law enforcement, civil society, academia, and the tech sector to examine the use of this technology and identify policies that will protect constitutional rights and values while also keeping us safe. In this report, our task force addresses some of the most vexing and important questions concerning facial recognition and provides recommendations to lawmakers and law enforcement on how they can address those concerns. With release of this report, we aim to assist lawmakers and law enforcement across the country in their efforts to keep the public safe while safeguarding vital constitutional rights.

Sarah Turberville  
*Director, The Constitution Project at POGO*



*Roughly half of all adults in the United States have pre-identified photos in databases used for law enforcement facial recognition searches.*

# I. Introduction

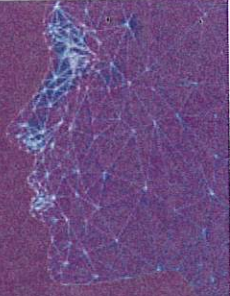
Imagine waking up one day to discover that the government required a license plate not just on cars, but also on you and every other person. A giant digital “Hello, My Name Is...” sticker floats above your head, identifying you to law enforcement everywhere you go. Not only that, these digital identifiers hovering over you have a bar code built in, allowing police to scan a photo and to catalog you in a crowd of tens of thousands of people, or instantly pull up a complete file about your life and activities.

Would you be worried to go outside with this name tag looming above you? Would you cautiously look out for and try to avoid cameras on the street? Would you try to veer away from a beat cop walking down the street in case they pull up your information and find an unpaid parking ticket? Would you hesitate to go to a psychiatrist, or a protest, or an Alcoholics Anonymous meeting knowing your identity would be broadcast to any video camera you pass by?

You don’t have to use your imagination to contemplate this world without anonymity. It’s already the type of reality we are creeping towards with facial recognition surveillance as it continues to be built into society without any rules or limits. Facial recognition technology has the power to eliminate anonymity and obscurity from American life. It could give the government greater surveillance powers than placing a police officer on every street corner.

While ever-watching facial recognition surveillance may seem like science fiction, the technology is very much part of today’s world. Half of all adults in the United States have pre-identified photos in databases accessible to law enforcement for facial-recognition searches, and a significant number of law enforcement entities possess the ability to use facial recognition for a range of surveillance and law-enforcement activities. However even as its power and prevalence grow, there are practically no laws limiting facial recognition surveillance. It’s time for that to change.

# II. Power and Use of Facial Recognition



## Defining Facial Recognition

Facial recognition is a method of using computer software to identify individuals based on the features of their face. These systems use facial “nodal points”—such as the location of eyes in relation to the face as a whole—from a pre-identified photo or set of photos to create a unique “face print” for an individual.<sup>1</sup> This face print acts as a baseline for an individual’s identification, and is used as a cross-check for identification against other photos or video footage. Facial recognition systems convert existing photos and photo databases into databases of face prints, and can use the prints in those databases to identify a large number of individuals.

Examining facial recognition requires distinguishing it from face matching (also called face verification) and face clustering, which have less severe privacy risks in their application.

Face matching is a similar but distinct computer technique in which software compares two images and answers a yes-or-no question as to whether the two faces are the same. Facial recognition, however, is a generalized identification tool that can provide an identification from millions of options. So while the technology employed to achieve face matching may be similar to facial recognition, face matching poses far less risk of harm to privacy and civil liberties.

Face clustering involves scanning a set of faces and using a computer program to categorize the individuals who are scanned based on certain features such as gender, ethnicity, or age range. For instance, face clustering could be used to track how many men and women shop at a store. Face clustering raises serious issues in application, including accuracy and potential for misuse. However, because it does not involve individualized identifications, face clustering does not raise the same kinds of risks addressed in this report.<sup>2</sup> Face matching and face clustering should be considered distinct from facial recognition as discussed in this report.

## How Facial Recognition Is Used

There are numerous ways law enforcement uses facial recognition technology. These different uses pose widely varying risks to constitutional and legal rights and will require varying regulation. Law enforcement use of facial recognition can be grouped into four primary purposes<sup>3</sup>:

- 1 *Arrest Identification*: When an individual is arrested and booked, police may use the mugshot photo taken during booking to later identify an individual who does not provide an identity, or to confirm an individual's identity.
- 2 *Field Identification*: Facial recognition is used by police officers working in the field to identify an individual they are speaking with; this could include discussions with a witness or victim of a crime, but is likely to primarily focus on identifying individuals that an officer stops during a patrol.
- 3 *Investigative Identification*: While investigating a crime, police may obtain the image of an unidentified suspect from a photograph or video footage; this could involve crime scene footage, or police covertly photographing an unidentified suspect they are actively watching. Law enforcement could then use facial recognition to identify the individual and further the investigation.
- 4 *Real-time surveillance*: This involves scanning all faces during a video feed and running them against a watchlist that will identify certain individuals. The contents of such a list could vary immensely; it could be limited to highly dangerous individuals that present immediate threats to public safety, or could be as broad as all individuals with a prior arrest for a minor crime.

## Development of Facial Recognition

Operational facial recognition technology only came into existence in the 1990s and did not see prominent law enforcement use until the 2001 Super Bowl.<sup>4</sup> There have been significant leaps in breadth of use of the technology in the intervening years. Most notably, the FBI ran over 52,000 facial recognition searches in fiscal year 2018, an average of over 4,000 searches per month.<sup>5</sup> Customs and Border Protection uses facial recognition for its biometric exit program to check the identity of individuals<sup>6</sup>—including citizens and lawful permanent residents—as they are boarding flights to leave the country, and the agency has announced plans to expand the program more broadly throughout

airports as well as seaports and land ports of entry into the United States.<sup>7</sup> Immigration and Customs Enforcement has discussed the purchase of facial recognition technology with vendors as well.<sup>8</sup>

Facial recognition is also widely available to and used by state and local law enforcement. According to the Center on Privacy and Technology at Georgetown Law, “at least 52 state and local law enforcement agencies that we surveyed were now using, or have previously used or obtained, face recognition technology...several other responsive agencies have opened their systems to hundreds of *other* agencies.”<sup>9</sup> (Emphasis in original) The 2016 Georgetown study estimates that at least one in four state or local police departments possesses the ability to run facial recognition searches either directly or via a partnering agency.<sup>10</sup>

## Key Factors

The power of facial recognition surveillance depends on three primary factors: 1) the capabilities of facial recognition software systems, 2) the size of databases of face prints that can be used to make identifications, and 3) the number and quality of cameras that can be used to obtain images of faces and scan them for identification. If each of these factors is at strength, the power of facial recognition surveillance can be immense. The most pervasive combination of these factors exists in China, which allows the government to quickly identify individuals over enormous geographic areas.<sup>11</sup> A BBC reporter testing China’s facial recognition dragnet was located in a city of 4.3 million people in a mere 7 minutes.<sup>12</sup> In the United States, the government has not deployed facial recognition surveillance at this level, but absent proper limits in law and policy, our nation may soon possess pervasive surveillance similar to the systems deployed in China.

### Software

For years companies have boasted facial recognition systems that can scan for a match against a set of tens of millions of pre-identified face prints.<sup>13</sup> The National Institute of Science and Technology (NIST) conducts annual testing of different facial recognition software systems, and the results confirm that the number of systems that can achieve a rapid level of identification and the speed of systems continue to grow.<sup>14</sup>

Despite advances, effectiveness of facial recognition scans varies greatly based upon situational factors. Image quality and the features that affect it—such as camera resolution, distance, lighting, angle—can impact accuracy,

and the quality of algorithms that examine and identify faces can vary widely. Setting different “confidence thresholds” for a system to register a match can impact effectiveness as well.<sup>15</sup> When facial recognition systems make an identification, they are technically providing a certain level of probability of a positive identification<sup>16</sup>; law enforcement entities are sometimes given the false impression that facial recognition provides definitive matches rather than merely probable matches,<sup>17</sup> a misconception that serves neither the police nor the public. Finally, facial recognition systems create serious misidentification issues, which we will discuss in more detail in the “Risks” section.<sup>18</sup>

Advances are also occurring in using facial recognition for real-time surveillance. Real-time facial recognition requires significantly more computational power than facial recognition systems that target, scan, and identify a single face, and is thus much more difficult to develop and deploy than targeted systems. Despite these difficulties, a March 2017 NIST report found that real-time facial recognition can be built.<sup>19</sup> We are beginning to see this in practice. Amazon currently markets a real-time facial recognition system called “Rekognition,” and the company boasts that in cities of operations such as Orlando its systems can continuously scan for “people of interest” using “cameras all over the city.”<sup>20</sup> According to a news analysis based on documents obtained from the Orlando police department:

Orlando PD uploads photos of “persons of interest” (officer volunteers) into the system; Rekognition analyzes their faces, maps their features, and indexes them. Then, faces from the city’s eight designated live video streams...are sent to Rekognition and compared against the Orlando-provided collection of faces. If the system detects a match between a pedestrian’s face and that of a “person of interest” in its index, it is supposed to instantly send a notification to police officers.<sup>21</sup>

The same situational factors that limit facial recognition’s effectiveness also apply to real-time systems. In fact, real-time facial recognition is limited to a higher degree, because when scanning a large number of faces and using live footage it is more difficult to obtain ideal image conditions for scans.

### ***Photo Databases***

Roughly half of all adults in the United States have pre-identified photos in databases used for law enforcement facial recognition searches.<sup>22</sup> The FBI maintains the largest network of photo databases that are accessed for facial recognition surveillance in the United States. Its Facial Analysis, Comparison, and Evaluation (FACE) Services Unit can search hundreds of millions of photos.<sup>23</sup>

The FBI's system is technically not a single, centralized database—it is built on agency-owned databases of mug shots, a broad range of civil service photos,<sup>24</sup> and millions of photos in databases of driver's licenses accessed through agreements with states.<sup>25</sup> States that permit the FBI to use their driver's license databases currently contain over 60 million licensed drivers.<sup>26</sup> These agreements aren't one way, either. Additionally, numerous state and local law enforcement entities have arrangements that let them use the FBI's database of mugshots and other photos. Other law enforcement agencies have built localized facial recognition systems of their own, capable of identifying millions of individuals. For example, Pennsylvania law enforcement uses a localized database composed of over 34 million DMV photos, and Florida law enforcement uses a database composed of over 45 million state DMV and mugshot photos.<sup>27</sup>

## **Camera Sources**

### **Closed-Circuit Television (CCTV)**

Although the United States does not have vast network of government CCTV cameras like China<sup>28</sup> or the United Kingdom,<sup>29</sup> it deploys cameras on a significant scale, especially in urban areas. The largest cities in the United States such as New York, Chicago, and Los Angeles all maintain a network of police CCTV cameras spread across the cities.<sup>30</sup> Chicago is particularly notable—its 30,000-camera network is massive.<sup>31</sup> Many smaller cities such as St. Louis<sup>32</sup> and New Orleans<sup>33</sup> have begun to develop networks of hundreds of CCTV cameras as well.

### **Police Body Cameras**

One of the biggest and ever-growing risks of mass government camera deployment in the United States comes from police body cameras. Over half of large police departments already use them,<sup>34</sup> including Chicago, Dallas, Los Angeles, Miami, New York City, Oakland, and Washington, DC.<sup>35</sup> While body camera programs are increasingly common, most departments were still in pilots or early stages of implementation as of 2016.<sup>36</sup> As body cameras become a common feature for all police officers, the number of law enforcement cameras in public will increase exponentially.

### **Privately Owned Cameras**

While government owned and operated cameras will likely be the primary source for photos and video footage used in facial recognition surveillance, it is also



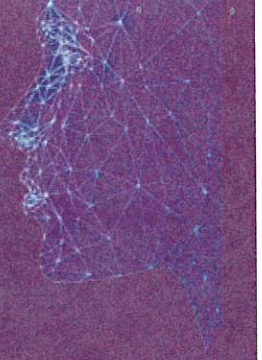
worth considering the impact of private sources. Police are increasingly using private CCTV and security cameras as a pre-built surveillance network, and asking individuals and businesses to formally register their cameras with police for use as part of centralized police monitoring systems.<sup>37</sup> With an estimated 30 million security cameras in the United States,<sup>38</sup> tapping into privately owned devices could allow the government to build a CCTV network on the scale of China (at least in terms of population ratio) at a fraction of the cost. And personal security cameras are rapidly expanding as a common consumer good, as is capability and desire by the government to connect cameras with law enforcement systems.<sup>39</sup>

### **Social Media Content**

Finally, social media platforms serve as some of the world's largest repositories of photos and videos. These platforms could be co-opted for investigative identification by accessing photos and scanning them in the same manner police would CCTV or body camera footage. In 2015, the surveillance service Geofeedia harvested data from social networking platforms for hundreds of law enforcement agencies, including scanning photos of protests to identify individuals participating in the demonstrations. After these disturbing practices were highlighted, Facebook, Instagram, and Twitter blocked Geofeedia's ability to harvest data from their platforms.<sup>40</sup> And recently Facebook disclosed that Russian firms building facial recognition systems for their government had scraped photos from Facebook to augment the Russian government's databases.<sup>41</sup> It is important that these and other social media companies maintain technical limits on API<sup>42</sup> access and scanning so that these commonly used consumer services do not become mass photo surveillance networks.

*Social media platforms could be co-opted for investigative identification by police accessing and scanning personal photos.*

# III. Constitutional Principles and Key Areas of Concern



Facial recognition technology creates unprecedented potential to monitor individuals, and thus unprecedented questions about how we should regulate surveillance technology. The technology takes one of the most basic human functions—the ability to recognize individuals by their appearance—and combines it with computer capabilities to act on a scale that would otherwise require massive amounts of human labor. This mix forces us to reconsider fundamental assumptions about how law enforcement can, and should, interact with individuals. It is critical that we carefully consider the impact on constitutional rights and principles, and proper limits of facial recognition surveillance, before allowing it to become a common law-enforcement tool.

Although policy debates are often framed as “privacy versus security” or “public safety versus civil liberty,” this divisive choice is rarely necessary. It is more often possible to find ways to isolate the harms from the benefits of new technologies and police tools, and to establish reasonable checks and limits that preserve the latter while guarding against the former. While facial recognition poses serious risks, it can also have substantial value. Facial recognition can simplify law enforcement activities, advance investigations, and identify wanted individuals who are at large. These benefits are considerable, and should not be needlessly sacrificed in the course of setting necessary limits on facial recognition in other areas. However, if the benefits are to be realized, it is essential that lawmakers create strong policies that eliminate the risks born from improper use and error.<sup>43</sup>

Some troubling potential applications of facial recognition may seem unlikely to be carried out by normal law enforcement officials who simply want to use these technologies to aid public safety. However, as is often the case with new technologies, a rush to application can often cause unintended harms and result in overbroad use. Even absent malicious application, it is important to alleviate concerns and prevent the chilling effects that surveillance can cause.

This requires considering risks not only in the context of what the government will do but also what it could do, and how fear of such potential actions may drive members of the public.

# Privacy and Fourth Amendment Protections

## *Privacy as a Vital Constitutional Principle*

Advances in digital technology have created unparalleled capabilities for collection, storage, cataloging, and use of sensitive data about individuals. Facial recognition surveillance is a prime example of this in every respect. By exploiting an ever-growing network of cameras, the government can apply facial recognition technology to video footage and photographs in a broad range of areas to identify individuals and collect data about their locations, activities, and interactions. Modern computers facilitate mass retention of this information, and allow for the creation of databases of hundreds of millions of photographs that can be used to create facial recognition profiles of the entire populace. Whereas just several years ago it was impossible for a police department of any size to comb through such vast databases and find matching faces in a timely manner, now facial recognition technology allows police officers to do so in seconds.

As a constitutional principle embodied in the Fourth Amendment's protection from "unreasonable searches and seizures," privacy is meant to do more than create legal walls that mirror physical ones, and is not limited to situations where we are inside our own houses or conducting conversations via phone or letter. Rather, privacy as a constitutional principle is meant to check a democratic government's power over its citizens; chiefly by limiting the amount of information it knows about us.<sup>44</sup> As Justice Sonia Sotomayor warned in her concurring opinion in *United States v. Jones*, permitting unrestricted use of innovative digital technologies that are "available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may alter the relationship between citizen and government in a way that is inimical to democratic society."<sup>45</sup>

In last year's landmark Supreme Court decision *Carpenter v. United States*, the Supreme Court took on the novel risks surveillance in the digital age pose, fully embracing the right to privacy. In an opinion focused on cellphone tracking, the Court declared that "the [Fourth] Amendment seeks to secure *the privacies of life* against arbitrary power"<sup>46</sup> (emphasis added), a framing that notably focuses not on certain places or types of conversation, but rather on protecting details of each person's life against an ever-watching government. Perhaps even more explicitly, the opinion of the Court in *Carpenter* stated that "a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance."<sup>47</sup>

Because the constitutional principle of privacy means placing checks on government power, it follows that privacy extends to some activities that take place in public.<sup>48</sup> When the Court in *Carpenter* highlighted that location records “hold for many Americans *the privacies of life*”<sup>49</sup> (emphasis added), it was emphasizing that Fourth Amendment privacy protections do not focus narrowly on privately owned places, but rather on people themselves, wherever they may be.

***Strong limits on surveillance technology will be necessary to properly rebalance power between the government and the people.***

The importance of limiting government access to the private lives of citizens is highest for sensitive information. But quantity of information can raise its own privacy issues. In *Carpenter*, the Court highlighted that “a cell phone—almost a feature of human anatomy—tracks nearly exactly the movements of its owner,” and therefore presents heightened risks to privacy.<sup>50</sup> While cell phones may have become an extension of our bodies, our faces require no such metaphor; unlike cellphones, our faces are never able to be turned off, left behind, or cast aside. If our faces can be subjected to the same type of continuous surveillance as cellphones, strong limits on surveillance technology will be necessary to properly rebalance power between the government and the people.

### ***Cataloging Sensitive Activities***

Facial recognition amplifies the concerns of upending privacy and unbalancing power between the government and its citizens in a unique and especially troubling way. The Supreme Court’s key fear in both *Jones* and *Carpenter* was that in the course of tracking location, the government would unearth individuals’ most sensitive activities. As Justice Sotomayor highlighted, this form of surveillance could catalog “trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.”<sup>51</sup>

Whereas GPS and cellphone tracking inevitably record individuals’ visits to these places, facial recognition surveillance could be directed at these

types of locations. A camera could be placed outside a mental health facility, a lawyer's office, a substance abuse treatment center, or myriad other sensitive locations, and, with facial recognition, government officials could compile a list of every individual who appears there. These individuals could be identified, or "metadata profiles" could simply be built, by creating face prints of people who engage in specific activities (for instance, "Addiction Clinic Attendee #371," "Firearm Store Shopper #746," "Planned Parenthood Visitor #925"), and stored en masse to be cross-checked and used at a later time. Using facial recognition in such a manner could allow the government to harvest information from broad video surveillance with minimal human labor and reduce that visual data to a form that is much more easily archived for potential later use.

Such data could be used for an immense array of future government activities, ranging from profiling, to selective law enforcement investigations, to applications for background checks, to evaluations for civil service employment opportunities.

Equally important is the potentially chilling effect on political and other types of participation, such as religious and community activities.<sup>52</sup> While it is difficult to measure the cause of inaction, research demonstrates that surveillance chills participation in basic activities.<sup>53</sup> This is particularly true of surveillance directed at sensitive activities and groups vulnerable to persecution.<sup>54</sup> If individuals believe that each camera on the street is cataloging every aspect of their daily lives, they may begin to alter their activities to hide from potential surveillance. That is something we must avoid, and we can do so through sensible reforms which demonstrate that checks against abuse are in place.

### ***Unchecked Location Tracking***

Facial recognition surveillance threatens to become as powerful a method of finding and tracking individuals as are cellphone and GPS tracking. While the Supreme Court has imposed a warrant requirement for these other forms of electronic location tracking,<sup>55</sup> no such limit exists for facial recognition. In time, facial recognition could become a uniquely powerful location-tracking tool because there is no "middle man" for government-managed cameras that controls access to the data; the entire surveillance system is managed and all relevant information is obtained directly by law enforcement. This makes independent checks and proper transparency and accountability all the more important.

Currently China is the only known nation that has sufficiently advanced facial recognition surveillance networks for location tracking.<sup>56</sup> One key difference limiting the US government's ability to do the same is the relatively lower number of cameras continuously recording the public.<sup>57</sup> However, as use of body cameras, CCTV, and public-private partnerships continue to expand,<sup>58</sup> the capacity to use facial recognition for location tracking will expand as well, especially if law enforcement is able to use the technology to circumvent the rules for electronic location tracking that the Supreme Court has created over the last decade.<sup>59</sup> Rather than demonstrating probable cause and obtaining judicial authorization to gather cellphone location data, officers may simply turn to facial recognition to bypass this process. This would undo well-established investigative procedural requirements, and risk abuse by removing independent oversight. Thus it is critical that legal standards for use of electronic location tracking be preserved as new technologies provide the same capacity for monitoring location that cellphones do today.

## **Prevalence of Misidentification**

Although facial recognition is capable of immense power, in certain situations its capabilities are also extremely limited. It is critical to examine these limits and respond accordingly, both to protect constitutional and legal rights and public safety.

### ***Facial Recognition Can Be Highly Inaccurate***

Perhaps the largest current risk facial recognition poses is misidentification. So long as this is a regular phenomenon for facial recognition, law enforcement use absent proper checks will put innocent individuals at risk of harm.

*Despite rapid advances, facial recognition must still grapple with serious challenges regarding misidentification.* Photos taken under ideal conditions—such as for a mugshot during a post-arrest booking—may be easier to pair with a face print, but photos or video footage taken in public are often subject to unsuitable conditions that reduce accuracy, such as poor and varying lighting, poor subject angle, moving subjects, and long and varying distances. This leads to “false positives,” where facial recognition systems indicate an identification that is actually false.<sup>60</sup> Ironically, investing in larger databases can actually cause more false positives by increasing the odds that a face with similar features registers a false match.<sup>61</sup> Unfortunately, law enforcement can

receive unrealistically optimistic information by vendors as to how well facial recognition works,<sup>62</sup> leading officers to be overly reliant on an identification source that, in reality, is limited in how it can be effectively deployed. 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.”<sup>63</sup> This description exaggerates what is possible, which can mislead law enforcement into believing facial recognition is a flawless super-tool rather than a limited technology with accuracy challenges in general and especially when applied with varying field conditions as described.

False positive rates are increased by the fact that some facial recognition systems are programmed to return the “closest” face print, rather than not return an identification if all face prints are below the designated threshold for matching.<sup>64</sup> Again, law enforcement officers may be oversold on what facial recognition programs are capable of; many will assume a software offering an identification match response means “identification match,” rather than “closest face the computer system could find, but by no means positive and it definitely needs verification.”<sup>65</sup>

Facial recognition is also less accurate for people of color and women. This raises serious risks that will be examined in more detail in the section on civil rights.

*Real-time facial recognition has especially high levels of misidentification.* Given that the technology is less accurate when unsuitable conditions are present, real-time facial recognition is much more prone to misidentifications. A study conducted by law enforcement in Wales of real-time facial recognition found that false positives occurred at a rate *over ten times* that of correct identifications.<sup>66</sup> An earlier study in Germany found similar accuracy problems, with overall accuracy rates averaging between 17 and 29 percent, and as low as 10 percent at night.<sup>67</sup> Thus while real-time facial recognition may be technically possible, it appears far removed from providing successful results—and, in fact, is likely to do more harm than good.

### ***Misidentification Creates Public Safety Risks***

Absent clear rules, verification processes, and necessary limits in certain situations, facial recognition could do more harm than good for public safety and law enforcement. Innocent individuals could be subject to police actions—in the case of use of force, this can lead to irreparable harm. If an

individual is improperly arrested because of facial recognition, they could be subjected to warrantless search, fingerprinting, inclusion in law enforcement databases, and detention, even if the error is quickly remedied. This would not only create public safety hazards, but also infringe on due process rights, which will be discussed in more detail in a separate section.<sup>68</sup>

Misidentification could harm law enforcement as well. Directing officers to investigate or arrest the wrong individuals could lead to significant misuse of resources. It is hard to imagine that systems which improperly flag ten individuals for every proper match, as was the case in the study of real-time surveillance, would increase the efficacy for officers. Perhaps even more damaging is the potential impact on police-community relations. If it becomes a common phenomenon for individuals to be improperly stopped, searched, and arrested based on the directions of a mistaken computer program, trust in law enforcement and willingness to engage with officers will decrease. Finally, misidentification would endanger officers since persons who have committed no crime and are not wanted for any criminal offense may be more likely to resist a well-intentioned but unjustified arrest. Misidentification as a result of facial recognition increases the probability of unnecessary confrontations.

Facial recognition may be useful, but only if proper checks guard against the damage misidentification can sow. The technology could be useful for post-arrest identifications, and as a tool to narrow suspects or confirm information during investigations. Notably, in these situations law enforcement can pursue ideal conditions for photos, and check responses against other data sources. However, using facial recognition as the basis for initiating immediate-response and street-level interactions, where real-time facial recognition with all its flaws would be deployed, is more likely to be counterproductive.

Facial recognition built into police body cameras is especially worrisome in this regard, because it would exacerbate all the risks posed by real-time facial recognition misidentifications. Officers would be expected to respond unilaterally and likely instantaneously to information from a facial recognition program, with no outside aid or necessary time to verify the software's response. The severity of these risks led Axon, one of the top producers of body cameras in the United States, to halt its years-long plans to build facial recognition into its device.<sup>69</sup>

Just as misidentification stems from a variety of causes, responding to it will require a number of actions. There should be effective minimum standards for the use of facial recognition, and strong restrictions for situations where facial recognition is less accurate, such as real-time surveillance. Facial recognition systems should not be the sole basis for police action; confirmation



requirements should be built into facial recognition systems before they are deployed. In situations where these necessary precautions are not or cannot be taken, facial recognition should not be instituted. And regular testing and auditing of facial recognition systems and law enforcement use of those systems will be necessary.

### ***Accuracy Problems Are Likely to Persist***

Some may dismiss misidentifications as only a temporary problem that will fade away, but as accuracy increases for certain uses of facial recognition, we are likely to see a broader application under new and less reliable circumstances. Using facial recognition to make identifications from police sketches<sup>70</sup> and as lie detectors<sup>71</sup> are already in discussion, despite such uses of facial recognition being more akin to junk-science than genuine investigative tools.

## **Equal Protection and Civil Rights**

Equal protection under law is one of the founding principles of American democracy, and became a constitutional principle in practice upon passage of the Fourteenth Amendment, which guaranteed equal protection to all Americans. Even after this, protecting civil rights has been a long and difficult fight, with the equal protection in its modern form coming into practice with the *Brown v. Board of Education* decision.<sup>72</sup> Since then equal protection rights have continued to evolve and grow, with courts and society gradually developing civil rights protections in various contexts, such as protection from discrimination on the basis of sex and sexual orientation. Society has also been forced to confront the civil rights ramifications of disparate impact. Government systems designed in a manner that disproportionately harm minorities can violate civil rights, even absent discriminatory intent.<sup>73</sup>

The government must continuously consider whether new policies and practices, especially those by law enforcement, have a disparate impact.<sup>74</sup> Historically, the US criminal justice system, including in its use of surveillance,<sup>75</sup> has discriminated against and had a disparate impact on marginalized communities, especially communities of color.<sup>76</sup> These inequities echo through today's criminal justice system, which still suffers from discriminatory bias and unfair policy differentials in many areas.<sup>77</sup> Even if facial recognition is designed and built to be accurate and unbiased, if surveillance systems incorporate it in a discriminatory manner then the technology is increasing the efficiency of an unjust system. Given the history

of discrimination in the criminal justice system, checks at every level are necessary to protect everyone's right to equal justice under law and to build public trust.

It is critical that the government consider equal protection rights and avoid the impact of these historic inequalities in the criminal justice system if it plans to use facial recognition technology. New technology-based law enforcement tools are often employed with the assumption that algorithms and artificial intelligence (AI) are incapable of bias. This assumption is wrong; research demonstrates advanced technologies can suffer from design flaws or employ existing social inputs that disproportionately harm people of color and religious minorities.<sup>78</sup> This problem is prevalent for facial recognition.

*Facial recognition is less accurate for people of color and women.* This year, an MIT Media Labs study found that error rates for computer systems using face images to recognize skin color and gender were significantly higher for people of color and women than for their white and male counterparts, with accuracy at its lowest for female people of color.<sup>79</sup> According to this study, even when these systems were able to correctly classify men with light skin 99 percent of the time, the same systems could only correctly classify women with dark skin as little as 65 percent of the time. Research by the American Civil Liberties Union (ACLU) has also found higher rates of misidentification for people of color.<sup>80</sup> Revelations of this problem are not new—a 2012 study co-authored by an FBI expert also warned that facial recognition was less accurate for people of color and women.<sup>81</sup> So just as facial recognition accuracy in general can be inflated, law enforcement might mistakenly infer from exaggerated descriptions that facial recognition is “colorblind.”<sup>82</sup>

These disparities in accuracy pose significant risks to equal protection and civil rights. If individuals from certain groups are erroneously identified as a suspect or dangerous, at-large criminal more often, these groups will inevitably be subject to undue harms. In addition to causing these direct harms, disproportionate error rates could plague police departments with “algorithmic bias,” whereby direct or implicit bias impacting how data are input into computer systems can cause bias in the system's results,<sup>83</sup> undermining police-community relations. It is also important to consider how higher misidentification rates will affect civil rights in other areas, such as public-sector employment: Erroneous misidentifications during an FBI background check could cause individuals to improperly be denied employment or promotions without recourse, and disproportionate error rates for people of color could cause systemic job discrimination.

Equal protection also requires clear and consistent standards for government action, especially punitive action. Development of surveillance tools should not lead to such broad police action that it might be carried out in an arbitrary or discriminatory manner. Yet facial recognition has already been deployed in some instances to target minority groups.<sup>84</sup>

*Facial recognition could exacerbate the disproportionate surveillance of minority communities, particularly people of color.* Existing disparities in surveillance systems and how they impact certain communities could be radically amplified by adoption of facial recognition surveillance. Marginalized groups are more likely to be subject to various forms of surveillance, including video surveillance networks that can be enhanced with facial recognition.<sup>85</sup> For instance, because African-Americans are disproportionately arrested and incarcerated,<sup>86</sup> they will disproportionately be included in mugshot databases used for facial recognition surveillance. As a result of these disparities, unrestricted facial recognition surveillance will likely have a far greater impact on people of color. The risk of this occurring makes it all the more essential that government develop sensible rules for facial recognition, and directly address how this technology will uniquely impact people of color.

## **Freedom of Expression and Association**

### ***Facial Recognition Endangers Anonymity and Obscurity***

The ability to freely participate in First Amendment-protected activities such as protests, political events, and religious ceremonies without disruption or discouragement is fundamental to American democratic society. Yet these activities could be subjected to facial recognition surveillance simply by placing government cameras nearby. And officers increasingly wear body cameras while on duty near protests, raising the question of whether body cameras' promised benefit of preventing misconduct or the risks of recording such sensitive activities are overriding.<sup>87</sup> The ability to rapidly identify every participant at such events raises the potential for disruption, and the ability to catalog all participants raises the specter of selective law enforcement action, or even overbroad prosecution.<sup>88</sup>

A necessary aspect of freedom of expression and association is group anonymity.<sup>89</sup> Over six decades ago, the Supreme Court held that "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."<sup>90</sup> In that case, *NAACP v. Alabama*, the key action at issue was the government demanding NAACP's Alabama membership list. In the digital age, no such direct action is necessary to remove the anonymity of an

organization's members. A single camera outside the entrance or exit to a group's events combined with facial recognition could produce a membership list without consent or even notification. And because such identification can be done with practically no expenditure of human resources, it can be conducted on a mass scale.

### ***Facial Recognition Endangers First Amendment Activities***

Facial recognition could be a tool to disrupt First Amendment-protected activities. Unrestricted, facial recognition could allow law enforcement to scan crowds during large protests, political events, or religious ceremonies, and then arrest any individual with an active bench warrant.<sup>91</sup> Ability to effortlessly identify any bench warrant for any petty offense could enable arbitrary action and abusive targeting, such as against selectively targeted individuals attending "events of interest," such as protests, political events, and religious ceremonies.

This was already observed on a small scale with Geofeedia—a social media-monitoring company—which admitted that Baltimore police used the service during protests to "run social media photos through facial recognition technology" to find individuals with "outstanding warrants and arrest them directly from the crowd," with the goal of targeting individuals who were protesting.<sup>92</sup> Given the number of bench warrants for petty offenses that some municipalities maintain, it is entirely possible that facial recognition could become an "arrest-at-will" authority used to disrupt such activities on a broad basis.

Facial recognition could be used to, without immediate interaction, catalog all participants at First Amendment protected activities such as protests, political events, and religious ceremonies. For instance, an FBI presentation on facial recognition highlighted its ability to identify participants at presidential campaign rallies.<sup>93</sup>

Facial recognition databases could also be developed based on First Amendment activities,<sup>94</sup> with participation in these activities then used for police investigations or in relation to civil service employment.

### ***Facial Recognition Could Chill First Amendment Activities***

Even if pernicious uses of facial recognition do not occur, the possibility—either from government policy or malicious individuals acting in absence of necessary checks and oversight—could create significant chilling effects. If individuals

believe that going to a protest could lead to a CCTV tagging them for arrest based on a years-old traffic ticket, they may choose to stay home instead. If someone fears attendees at a Muslim student event are being cataloged via facial recognition the same way “Mosque crawlers” who were recruited to participate in and spy on Muslim community events tried to build such lists for the NYPD Muslim surveillance program, they may avoid engaging with their religious community.<sup>95</sup>

Such fears of and capabilities for abuse must be put to rest. Requiring independent authorization for facial recognition will serve as a critical means of preventing improper use, and of assuring the public that this powerful surveillance tool is properly limited. Limiting facial recognition to serious crimes would also prevent abuse, and additionally stop facial recognition from being used to create arrest-at-will authority for the type of selectively targeted activity against protestors that Geofeedia described.

### ***Facial Recognition Endangers Press Freedoms***

A free and functional press cannot be subject to overbroad surveillance. Congress has long established special protection for journalists concerning the search and seizure of their documents.<sup>96</sup>

Forty states and the District of Columbia maintain shield laws that offer a degree of privilege to journalists to protect their sources.<sup>97</sup> Nonetheless, at-risk sources such as whistleblowers often take extraordinary measures to ensure the secrecy of their interactions, including eschewing even the most secure forms of electronic communication in favor of in-person meetings to avoid potential electronic surveillance.<sup>98</sup> Modern surveillance powers force journalists to take extra precautions, such as leaving cell phones and other electronic devices with built in GPS at home. But facial recognition can be used not just to catalog activities, but also interactions. If it becomes a tool to pinpoint how individuals interact and meet with journalists, it

***It is critical that the government consider equal protection rights and avoid the impact of these historic inequalities in the criminal justice system if it plans to use facial recognition technology.***

could present significant roadblocks for journalists seeking to speak to sources and whistleblowers while preserving anonymity.

## **Due Process and Procedural Rights**

### ***Facial Recognition Could Undermine Requirements for Police Action***

Protecting due process rights requires ensuring that new technology does not circumvent rules and requirements for investigative or police actions, which are strictly limited by due process requirements and must be based on proper suspicion. Whether governing stop-and-frisks, investigations, searches, arrests, or uses of force, it is critical that existing checks and limits are preserved as the new law enforcement tools dramatically change the basis for and nature of these actions.

Yet, due process protections could be subverted by facial recognition. Because facial recognition makes probabilistic findings (meaning the software chooses images that have a higher but not certain probability of being correct),<sup>99</sup> relying on it could create impossible questions of what algorithmic thresholds sufficiently constitute suspicion or danger in relation to various investigative or police actions (such as stop-and-frisks) designating individuals as suspects, and arrests. Further, the ability to invoke facial recognition as the cause for police action and investigative decisions could create a troubling perverse incentive to use software with higher rates of false positives. If alerting police officers to a facial recognition match—regardless of whether the match ultimately proves to be correct—is deemed sufficient to justify investigative actions, then systems with high rates of positive identification could be more commonly adopted as they make investigative actions more readily available.

New technologies can often outpace law and policy guidelines. This has already occurred in regard to location tracking: By the time the Supreme Court ruled in 2012 that attaching GPS devices to cars required a warrant—based on a case originating in 2005—law enforcement had already redirected location tracking tactics to cell phone tracking, which in turn existed in a state of legal limbo until 2018.<sup>100</sup> Now facial recognition could offer a new means of tagging locations and tracking movements and reset the cycle again. These new technologies must not be treated as shortcuts that work around legal requirements. Doing so undermines both individual rights and police-community relations.

## ***Facial Recognition Could Damage Evidence and Defendants' Rights***

Protecting due process rights also requires ensuring evidence—both direct and derivative<sup>101</sup>—obtained from new surveillance technologies is subject to evidentiary and disclosure rules. New surveillance technologies are sometimes hidden from the public and defendants, either by arguing that contract rules and nondisclosure agreements prevent revealing their existence,<sup>102</sup> or by using “parallel construction,” in which the method of obtaining evidence is obfuscated by creating and reporting an alternate discovery technique.<sup>103</sup> This seriously undermines due process rights, notably the ability to challenge potential improper evidence collection, as well as constitutional requirements for disclosure of exculpatory evidence established in *Brady v. Maryland*.<sup>104</sup> It's critical for due process and public trust that the government respect the importance of defendants' access to evidence, including evidence involving the use of facial recognition surveillance.

Unfortunately, facial recognition surveillance is often shrouded in secrecy. In Pinellas County, Florida, law enforcement used facial recognition technology for 15 years without ever providing the public defender's office any indication of its use in *Brady* or discovery disclosures.<sup>105</sup> Amazon designed a non-disclosure agreement with law enforcement for its facial recognition systems to prevent disclosure of a product roadmap describing how its systems could be used,<sup>106</sup> raising the specter of the government repeating its misuse of NDAs to hide broad use of cell-site simulators (more commonly called “stingrays”) for years.<sup>107</sup>

Protecting due process rights and preserving *Brady* rights<sup>108</sup> also requires that the government disclose not only the use of facial recognition but also how reliable its systems are. Unlike other forms of forensic evidence such as DNA testing, facial recognition is highly variable in its dependability. A facial recognition system that leads to police action could be either reasonably accurate or highly unreliable based on a range of factors, such as the algorithm employed, the confidence thresholds used to trigger a match, the dataset of face prints used, and the demographic composition of that set. Merely disclosing the use of facial recognition without providing details about that system's accuracy, confidence thresholds employed, or other factors would be akin to prosecutors disclosing that they based an investigation on an eyewitness account, but refusing to say how far away the witness was, or submitting a fingerprint match into evidence without letting defense counsel cross-examine the expert who made that determination. In order for proper evidence disclosure in relation to facial recognition to have any impact, accuracy of systems employed must be made known, and subject to questions and challenges in court.

## Transparency and Accountability

All too often new surveillance technologies, including those that can “alter the relationship between citizen and government in a way that is inimical to democratic society,”<sup>109</sup> are adopted without public consent or awareness. This undercuts democratic governance, and damages public trust in government.

It is critical that the public know the details on how facial recognition is deployed and how it functions.<sup>110</sup> This includes disclosing what type of computer programs are being used, what vendors are being employed, and the details on policies for database development and use. Additionally, properly informing the public necessitates testing for accuracy, both in general and for specific demographics and situations, as well as conducting audits on how facial recognition is used. However, as described in the previous section, the government is not currently conducting such oversight.<sup>111</sup>

Maintaining transparency for surveillance programs is not only important for ensuring public trust but also critical to protecting the principles discussed above. Protecting privacy requires shining a light on how surveillance is used in order to prevent abuse and stop certain activities from being chilled. Equal protection requires studying whether facial recognition affects certain groups in different ways or exposes them to improper police action based on misidentification. Protecting freedom of expression requires public rules and auditing to demonstrate the rules are being followed. Due process entails disclosure of the uses of facial recognition and of details about specific software used and its accuracy. And it is impossible to understand the impact facial recognition will have on public safety without examining the details of how accurate the technology is and the manner in which law enforcement uses it.



# IV. Recommendations

The following recommendations are intended to guide policymakers in considering how to properly regulate facial recognition surveillance in a manner that both protects constitutional principles and aids public safety. While they are primarily meant to guide Congress and state legislatures in crafting legislation, we believe these recommendations would have significant positive effects if adopted by police departments and law enforcement agencies as well.

There are several important general items to note in relation to our recommendations. First, for all recommendations that involve judicial authorization such as warrants, exigent-circumstances exceptions will apply under Fourth Amendment law; thus, the recommended checks on facial recognition are not likely to hamper emergency responsiveness. Second, principles of federalism should be followed to ensure that states and localities can enact stronger protections that are not pre-empted. Any federal law adopted based on these recommendations should not prohibit states and localities from enacting stronger protections against facial recognition surveillance, including full prohibitions on the use of the technology within a particular state or locality. And third, all of the recommended rules and limits should apply to vendors, contractors, and other private entities that act as law enforcement agents with respect to facial recognition surveillance, including those that engage in data storage and data mining.

## **1. Require judicial authorization based upon probable cause for using facial recognition for identification**

Independent judicial authorization should exist as a check on facial recognition surveillance that allows the technology to provide the greatest benefit to law enforcement—rapidly identifying individuals filmed or photographed in the commission or fleeing the scene of a crime—without subjecting the general populace to this invasive surveillance tool. The law should require:

- The government to first obtain judicial authorization whenever it seeks to use facial recognition to identify an individual.
- That this judicial authorization be based on a probable-cause

determination that the individual has committed, is committing, or is about to commit a crime.<sup>112</sup>

- That exceptions exist for exigent circumstances, victims, and missing persons, and obtaining and confirming an individual's identify during post-arrest booking.
- That exceptions exist for in-person "Field Identifications" after an officer has stopped an individual, the officer be required to have probable cause that the individual has committed, is committing, or is about to commit a crime in order to use facial recognition to determine or verify that individual's identity.<sup>113</sup>
- That the judicial authorization process include exhaustion requirements and minimization rules similar to those for wiretaps, and an exclusionary rule for evidence obtained using facial recognition surveillance without compliance with these procedures.

These policies address a number of the risks described above. Most notably, they would establish an independent check to prevent facial recognition from being misused against individuals not suspected of wrongdoing. This will both prevent abuse of power and assure individuals that their daily activities are not being monitored and cataloged. Additionally, these policies would prevent facial recognition surveillance from circumventing investigative requirements for electronic location tracking.

## **2. Require judicial authorization based upon probable cause for using facial recognition to catalog activities**

The government should be prevented from building mass databases of location and association information based on facial recognition scans that can be accessed later without limitation. The law should require:

- That the government first obtain judicial authorization whenever it seeks to use facial recognition to create a profile that identifies the locations, activities, or interactions of the person rather than a name.
- That this judicial authorization be based on a probable cause determination that the individual has committed, is committing, or is about to commit a crime.<sup>114</sup>

Absent these policies, the government could regularly scan locations and events and tag every individual without identifying them by name, save and update these profiles, and then refer back and use this stockpile of data to match a

recorded profile once an individual becomes a person of interest. Creation of mass databases of these “metadata profiles” would severely undermine privacy, and risk chilling public participation in sensitive activities. Implementation of these recommendations would stave off such harms, while still permitted permitting the use of facial recognition to catalog associational activities directly involving crimes, such as suspected communications made as part of a conspiracy.

### **3. Limit use of real-time facial recognition to emergency situations**

While real-time facial recognition is promising in theory, in practice the high level of inaccuracy and challenges that will be likely when scanning images in field conditions pose serious risks. Innocent individuals could be subject to improper police actions including arrest and use of force if real-time scans of crowds with facial recognition software become common practice. As a corollary, police-community relations could decline as all individuals fear that a computer error may lead an officer to target them improperly. Therefore, real-time facial recognition should be limited to emergency situations.

- Real-time facial recognition should only be permitted to scan for individuals when a senior law enforcement official (we recommend this be a state’s Attorney General or, for federal law, the U.S. Attorney General) has signed a written authorization that they believe the presence of such individual in a designated area constitutes exigent circumstance.
- Within 24 hours of beginning real-time facial recognition scanning, government officials demonstrate to a court that the presence of such individuals at the designated area constitutes emergency circumstances.
- Real-time scanning for such individuals be discontinued as soon as the described emergency circumstances no longer exist, or within 72 hours; government officials may return to court to receive continuation approval for additional 72-hour periods as necessary.

### **4. Limit facial recognition surveillance to serious crimes**

Whenever law enforcement uses facial recognition for any purposes other than post-arrest identification, its use should be limited to serious crimes. Specifically:

- Law enforcement use of facial recognition should be limited to

preventing, investigating, and prosecuting Uniform Crime Reporting Title 1 crimes (homicide, rape, robbery, aggravated assault, burglary, larceny, arson).

- Kidnapping and child exploitation crimes should be included as serious crimes for which law enforcement can use facial recognition.
- In terms of the property crimes listed above, burglary should be limited to first degree burglary, and larceny should only apply to crimes involving theft of property of at least \$1,000 in value.
- Crimes that necessarily include the above crimes in their commission should also be included.

## **5. Require independent verification for facial recognition identifications before allowing them to serve as the basis for police action**

Facial recognition can aid law enforcement activities, but it is by no means infallible and shouldn't be treated as such. Ideally, law enforcement officers will understand the limits of facial recognition technology and systems will be programmed to provide probabilistic findings. But it is still essential that laws set out clear and unambiguous rules that will pre-empt improper action based on facial recognition, and also serve to guide officers in proper procedures for relying on an unprecedented technology. The best way of requiring independent verification and of effectively building facial recognition into existing law enforcement procedures is to assign a measure of reliability and evidentiary value to facial recognition matches<sup>115</sup>:

- For field identifications (when an individual is already stopped and is being identified) and investigative identifications, a facial recognition match should be treated as equivalent to receiving information from a confidential informant in terms of its reliability and evidentiary value in building suspicion or cause for further police action.
- If a facial recognition match is being used as the basis for an immediate action in the field such as a Terry stop (also known as a "stop and frisk") or arrest—which is most likely to occur in reaction to real-time facial recognition—such a match should be treated as equivalent to receiving an anonymous 911 call from an informant in terms of its reliability and evidentiary value in building suspicion or cause for further police action.

In addition, investigations should designate separate officers to conduct facial recognition searches and restrict direct participation by officers overseeing

the relevant investigation to avoid tainting either the facial recognition search results or ongoing investigative activities. All officers that use facial recognition or are prompted to act based on a facial recognition match should be trained in the use of the technology and its limits to reduce confirmation bias in field activities.

## **6. Place a moratorium on real-time facial recognition built into body cameras**

The serious risks posed by real-time facial recognition will be exacerbated if this technology is incorporated into police body cameras. Facial recognition built into body cameras would create the serious risk of isolating officers, forcing them to make unilateral decisions prompted by an unreliable computer system. Given the heightened possibility of misidentifications by real-time facial recognition, this would put the public at greater risk of misidentifications, and lead officers to make incorrect decisions that reduce law enforcement efficiency and harm police-community relations. Therefore, we recommend:

- An indefinite moratorium on incorporating real-time facial recognition systems into police body cameras.
- That body camera footage uploaded at the end of an officer's shift into a law enforcement database for later review be treated similarly to footage from other law enforcement cameras, such as CCTV.

Because storing body-camera footage will dramatically increase the amount of video available to law enforcement for facial recognition uses and will likely impact how members of the public interact with officers wearing body cameras, any department that uses facial recognition on body camera footage after it is uploaded should have clear and effective policies governing the use of body cameras and recorded footage.<sup>116</sup>

## **7. Establish standards for transparency and testing**

Facial recognition's reliability is largely dependent upon the use of standards; accuracy can vary widely based on the quality of the software, confidence thresholds, the nature of databases, and circumstances under which images are taken. It is essential that if law enforcement is going to use facial recognition technology, it is of a sufficiently high quality to ensure accuracy. Further, it is also critical that the public have a clear understanding of how facial recognition is being used.

- Any law enforcement entity using facial recognition should submit its systems to independent testing.
  - ▶ Testing should be conducted by an independent entity with experience and expertise, such as the National Institute on Standards and Technology.
  - ▶ Testing should examine different field conditions, and evaluate accuracy both in general and in relation to specific demographic characteristics—such as ethnicity and gender—alone and in combination. For example, law enforcement agencies should test for differences in accuracy when the system attempts to identify an older Caucasian man versus when it attempts to identify a young African-American woman.
- Law enforcement agencies should only be permitted to use facial recognition after meeting pre-established minimum standards of accuracy set by the agency designated to conduct testing, both in general and for specific demographics.
- The entity conducting tests should publicly disclose the test results.
- Periodic reporting on use should be compiled and publicly issued.
  - ▶ These reports should include information such as how often the technology is used, court orders are sought and obtained, and exigent circumstances are invoked.
  - ▶ These reports should also include the results of regular audits conducted to ensure compliance with rules governing the use of facial recognition technology.

## **8. Provide notice to criminal defendants**

It is critical that defendants have the right to examine and challenge, both in terms of legality and accuracy of process, how evidence developed—this right should apply to facial recognition surveillance just as it does to traditional investigative activities and forms of evidence collection.

- All law enforcement uses of facial recognition should be disclosed to criminal defendants prior to trial.
- Such disclosure should include the use of facial recognition as a direct source of evidence and whenever it was the basis of derivative evidence in the defendant's case.
- Disclosure of use of facial recognition should include descriptions of

technical features such as the vendor employed, confidence thresholds, and the manner in which results are presented (such as details included within a candidate list of potential matches).

- The government should be required to explain in court the reliability of any facial recognition systems it used, and defendants should be given the opportunity to question a law enforcement official on any aspect of the facial recognition system's features that might cause doubt as to the reliability of results.

## **9. Establish rules for sharing access across government agencies**

Effective rules for facial recognition surveillance will mean little if a government agency can simply sidestep them by using another agency that is not bound by these rules, or by providing data that empowers other government entities to engage in unrestricted facial recognition surveillance. As discussed, many facial recognition systems—especially the system used by the FBI in connection with state photo databases—depend upon data collected by other government entities. Consistent rules and practices should govern the sharing of information to aid in facial recognition surveillance.

- If a federal, state, or local law or policy enacts any of the above recommendations or any other limits on facial recognition surveillance, these limits should also apply to covered departments' and agencies' ability to share tools or data with other entities for facial recognition surveillance. Government entities should only share data—such as that gleaned by conducting scans, or information obtained by providing access to photo databases—and tools with any other government entity if that entity is bound by equally strong rules and limits on facial recognition surveillance.

.....

**Explanatory Statement of Thomas Nestel:**

*I support the Task Force's recommendations, including those requiring independent judicial authorization as a check on facial recognition surveillance found throughout this report. I believe that wiretaps should be held to a uniquely high standard in terms of exhaustion and minimization rules, as described in the report. However, I do not think facial recognition should have identical exhaustion and minimization rules. I also believe court approval for use of facial recognition for the specific purpose of cataloguing activities should be centered on law enforcement access to such information, rather than the initial collection. Along with the Task Force, I support limits on the use of real-time facial recognition, although I think real-time facial recognition should also be available to respond to pre-existing arrest warrants for serious crimes—but only if the human review requirements we put forward in Recommendation 5 are satisfied. I would also permit facial recognition (within the limits set forth throughout the report) to be used in the case of sexual assault and larceny of \$500 or more in value, along with the serious offenses listed in Recommendation 4.*

.....



# Endnotes

- 1 Neural networks, a machine-learning technique that uses a large quantity of prior analysis and data to develop skillsets, have become a common element of facial recognition software in recent years, dramatically increasing facial recognition's power and capabilities. Tajha Chappellet-Lanier, "Facial recognition algorithms are getting a lot better, NIST study finds," *FedScoop*, December 3, 2018. <https://www.fedscoop.com/facial-recognition-algorithms-getting-lot-better-nist-study-finds/> (Downloaded January 6, 2019)
- 2 For more information, see Section IV, Recommendations.
- 3 See Clare Garvie et al., "The Perpetual Line-Up: Unregulated Police Face Recognition in America," Center on Privacy & Technology at Georgetown Law, October 18, 2016 pp. 10-12. <https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf> (Hereinafter Perpetual Line-Up Report) (Downloaded January 6, 2019)
- 4 Jennifer Tucker, "How facial recognition technology came to be," *The Boston Globe*, November 23, 2018. <https://www.bostonglobe.com/ideas/2014/11/23/facial-recognition-technology-goes-way-back/CkWaxzovFcveQ7kvdLHGI/story.html>; Jesse Davis West, "A Brief History of Facial Recognition," FaceFirst, August 1, 2017. <https://www.facefirst.com/blog/brief-history-of-face-recognition-software/>; Kaleigh Rogers, "That Time the Super Bowl Secretly Used Facial Recognition Software on Fans," *Motherboard*, February 7, 2016. [https://motherboard.vice.com/en\\_us/article/kb78de/that-time-the-super-bowl-secretly-used-facial-recognition-software-on-fans](https://motherboard.vice.com/en_us/article/kb78de/that-time-the-super-bowl-secretly-used-facial-recognition-software-on-fans) (Downloaded January 6, 2019)
- 5 In Fiscal Year 2018, the number was 4,325. Federal Bureau of Investigation, "November 2018 Next Generation Identification (NGI) System Fact Sheet," <https://www.fbi.gov/file-repository/ngi-monthly-fact-sheet/view>; Government Accountability Office, *Face Recognition Technology: The FBI Should Ensure Better Privacy and Accuracy*, (GAO-16-267), May 2016, p.49. <http://www.gao.gov/assets/680/677098.pdf> (Downloaded January 6, 2019)
- 6 Frank Bajak and David Koenig, "Face scans for US citizens flying abroad stirs privacy issues," *Associated Press*, July 12, 2017. <https://apnews.com/acf6bab1f5ab4bc59284985a3babdca4> (Downloaded January 6, 2019); This system uses the photos from the flight manifest of passengers

to create its full set of pre-identified face prints to scan for, a very small sample size. Therefore, while it is technically facial recognition, the current program is more akin in its impact to face matching because of its small scale and because the goal is to verify individuals boarding as pre-identified passengers. However there are no assurances this system or future iterations will not expand to broader database scans.

- 7 Dami Lee, "TSA lays out plans to use facial recognition for domestic flights," *The Verge*, October 15, 2018. <https://www.theverge.com/2018/10/15/17979688/tsa-precheck-facial-recognition-airport-cbp-biometric-exit> (Downloaded January 6, 2019); Calvin Biesecker, "CBP Set To Begin Face Recognition Evaluations Of Pedestrians, Vehicle Occupants At Land Ports," *Defense Daily*, June 28, 2018. <http://www.defensedaily.com/cbp-set-begin-face-recognition-evaluations-pedestrians-vehicle-occupants-land-ports/> (Downloaded January 6, 2019); "IDEMIA Tech Aids CBP Trial of Biometric Screening at Sea Port," *Find Biometrics*, November 14, 2017. <https://findbiometrics.com/idemia-cbp-biometric-screening-sea-port-411144/> (Downloaded February 8, 2019).
- 8 Jake Laperruque and Andrea Peterson, "Amazon Pushes ICE to Buy Its Face Recognition Surveillance Tech," *The Daily Beast*, October 23, 2018. <https://www.thedailybeast.com/amazon-pushes-ice-to-buy-its-face-recognition-surveillance-tech> (Downloaded January 6, 2019)
- 9 Perpetual Line-Up Report, p. 15.
- 10 Perpetual Line-Up Report, p. 25.
- 11 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> (Hereinafter China's Dystopian Dreams) (Downloaded January 6, 2019)
- 12 Jon Russell, "China's CCTV surveillance network took just 7 minutes to capture BBC reporter," *TechCrunch*, December 13, 2017. <https://techcrunch.com/2017/12/13/china-cctv-bbc-reporter/> (Downloaded January 6, 2019)
- 13 Francis Bea, "Goodbye, Anonymity: Latest Surveillance Tech Can Search Up to 36 Million Faces Per Second," *Digital Trends*, March 25, 2012. <https://www.digitaltrends.com/cool-tech/goodbye-anonymity-latest-surveillance-tech-can-search-up-to-36-million-faces-per-second/> (Downloaded January 6, 2019)
- 14 Patrick Grother et al., *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification*, National Institute of Standards and Technology, November 27, 2018. <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf>; National Institute of Standards and Technology, "Face Recognition Vendor Test (FRVT) 1: N 2018 Evaluation." <https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-1n-2018-evaluation> (All downloaded January 6, 2019)
- 15 "Thresholds allow you to tweak a face recognition system based on the degree of accuracy you desire for your individual-use case. The likelihood of

a match can be increased by implementing a low threshold, as in the case of identifying amusement park goers for their roller coaster photo souvenir— or decreased by implementing a high threshold, as in the case of banking transaction verification.” Ben Virdee-Chapman, “The Secret to Better Facial Recognition Accuracy: Thresholds,” Kairos, September 27, 2018. <https://www.kairos.com/blog/the-secret-to-better-face-recognition-accuracy-thresholds>; Employing different confidence thresholds can dramatically impact frequency of erroneous matches. American Civil Liberties Union, “ACLU Comment on New Amazon Statement Responding to Facial Recognition Technology Test,” July 27, 2018. <https://www.aclu.org/news/aclu-comment-new-amazon-statement-responding-face-recognition-technology-test> (Hereinafter, “ACLU Rekognition Comment”) (Downloaded January 6, 2019)

- 16 “Face recognition is inherently probabilistic: It does not produce binary ‘yes’ or ‘no’ answers, but rather identifies more likely or less likely matches. Most police face recognition systems will output either the top few most similar photos or all photos above a certain similarity threshold.” Perpetual Line-Up Report, p. 9.
- 17 For example, vendor FaceFirst greatly exaggerates when it claims 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.” Jesse Davis West, “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/> (Hereinafter Cost of a False Arrest); Cognitec states that “Face recognition is *a highly efficient tool* supporting law enforcement agencies to identify suspects.” (emphasis added) Cognitec, “Applications: Law enforcement.” <http://www.cognitec.com/applications-law-enforcement.html>; and Dataworks Plus promises 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 characteristics of the facial image” with capabilities such as “*discovering a person’s identity* during investigations.” (emphasis added) Dataworks Plus, “Facial Recognition Technology & Case Management.” <http://www.dataworksplus.com/faceplus.html> (All downloaded January 6, 2019)
- 18 For more information, see Section III, “Prevalence of Misidentification.”
- 19 Patrick Grother, et al., *Face In Video Evaluation (FIVE) Face Recognition of Non-Cooperative Subjects (NISTIR 8173)*, National Institute of Standards and Technology, March, 2017. <http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8173.pdf> (Downloaded February 8, 2019)
- 20 Matt Cagle and Nicole Ozer, “Amazon Teams Up With Government to Deploy Dangerous New Facial Recognition Technology,” American Civil Liberties Union, May 22, 2018. <https://www.aclu.org/blog/privacy-technology/>

- [surveillance-technologies/amazon-teams-government-deploy-dangerous-new](#)  
(Hereinafter ACLU Rekognition Blog Post) (Downloaded January 6, 2019)
- 21 Davey Alba, "With No Laws To Guide It, Here's How Orlando Is Using Amazon's Facial Recognition Technology," *BuzzFeed News*, October 26, 2018, updated October 30, 2018. <https://www.buzzfeednews.com/article/daveyalba/amazon-facial-recognition-orlando-police-department>. (Hereinafter Orlando Use of Facial Recognition) (Downloaded January 6, 2019)
- 22 Perpetual Line-Up Report, p.8.
- 23 Perpetual Line-Up Report, pp. 13-14.
- 24 This includes "photos submitted for licensing, employment, security clearances, military service, volunteer service, and immigration benefits." Government Accountability Office, *Face Recognition Technology: The FBI Should Ensure Better Privacy and Accuracy*, (GAO-16-267), May 2016, p. 11. <http://www.gao.gov/assets/680/677098.pdf> (Downloaded January 6, 2019)
- 25 Specific agreements vary—in some states the FBI maintains the ability to directly access and use state DMV databases for its facial recognition systems, while in others the FBI sends requests that are directly carried out by state entities. Testimony of Diana Maurer, Government Accountability Office, "Testimony, Before the Committee on Oversight and Government Reform, House of Representatives: Face Recognition Technology: DOJ and FBI Need to Take Additional Actions to Ensure Privacy and Accuracy," March 22, 2017, pp. 2-4. <https://www.gao.gov/assets/690/683549.pdf> (Hereafter, "GAO Testimony") (Downloaded February 8, 2019)
- 26 GAO Testimony, p.1.
- 27 Perpetual Line-Up Report, pp. 31, 51, 131.
- 28 Chinese state news boasts that Beijing's CCTV network is so pervasive that cameras are watching "every corner" of the city. Vivienne Zeng, "Every corner' of Beijing covered by surveillance cameras, state media proudly announce," *Hong Kong Free Press*, October 5, 2015. <https://www.hongkongfp.com/2015/10/05/every-corner-of-beijing-covered-by-surveillance-cameras-state-media-proudly-announce/> (Downloaded January 6, 2019); China deploys an estimated total of over 200 million government CCTV cameras. China's Dystopian Dreams.
- 29 "The UK is one of the most surveilled nations in the world. An estimated 5.9 million CCTV cameras keep watch over our every move." James Temperton, "One nation under CCTV: the future of automated surveillance," *Wired*, August 17, 2015. <https://www.wired.co.uk/article/one-nation-under-cctv> (Downloaded January 6, 2019)
- 30 American Civil Liberties Union, "What's Wrong With Public Video Surveillance?." <https://www.aclu.org/other/whats-wrong-public-video-surveillance> (Downloaded January 6, 2019)

- 31 Timothy Williams, "Can 30,000 Cameras Help Solve Chicago's Crime Problem?" *The New York Times*, May 26, 2018. <https://www.nytimes.com/2018/05/26/us/chicago-police-surveillance.html> (Downloaded January 6, 2019)
- 32 Danny Wicentowski, "Inside St. Louis' Real Time Crime Center, Cameras, Cameras Everywhere," *The Riverfront Times*, May 23, 2018. <https://www.riverfronttimes.com/newsblog/2018/05/23/inside-st-louis-real-time-crime-center-cameras-cameras-everywhere> (Downloaded January 6, 2019)
- 33 Jeff Adelson, "New Orleans' latest weapon in fighting crime? Surveillance cameras with big blue, red flashing lights," *The New Orleans Advocate*, January 27, 2018. [https://www.theadvocate.com/new\\_orleans/news/crime\\_police/article\\_ef983ae2-03a4-11e8-9d9e-437e9ffae9d1.html](https://www.theadvocate.com/new_orleans/news/crime_police/article_ef983ae2-03a4-11e8-9d9e-437e9ffae9d1.html) (Downloaded February 5, 2019)
- 34 Rachel Lerman, "Body cameras now in half of the big city police departments," *Seattle Times*, July 8, 2016. <https://www.seattletimes.com/business/technology/body-cameras-now-in-half-of-big-city-police-departments/>
- 35 The Leadership Conference on Civil and Human Rights and Upturn, *Police Body Worn Cameras: A Policy Scorecard*, (Version 3.04), November 2017, pp. 2-4. <https://www.bwcscorecard.org/static/pdfs/LCCHR%20and%20Upturn%20-%20BWC%20Scorecard%20v.3.04.pdf> (Downloaded January 6, 2019)
- 36 Mike Maciag, "Survey: Almost All Police Departments Plan to Use Body Cameras," *Governing*, January 26, 2016. <http://www.governing.com/topics/public-justice-safety/gov-police-body-camera-survey.html> (Downloaded January 6, 2019)
- 37 Faith Karimi, "Home surveillance cameras are the new neighborhood watch," *CNN*, August 31, 2018. <https://www.cnn.com/2018/08/30/us/home-surveillance-cameras-neighborhood-watch/index.html> (Downloaded January 6, 2019)
- 38 James Vlahos, "Surveillance Society: New High-Tech Cameras Are Watching You," *Popular Mechanics*, September 30, 2009. <https://www.popularmechanics.com/military/a2398/4236865/> (Downloaded January 6, 2019)
- 39 "[Amazon's patents] consider ways of using Ring's devices to recognize 'suspicious' people in a neighborhood and then automatically alert law enforcement." Ben Fox Rubin, "Amazon's Ring takes heat for considering facial recognition for its video doorbells," *CNET*, December 14, 2018. <https://www.cnet.com/news/amazons-ring-takes-heat-for-considering-facial-recognition-for-its-video-doorbells/> (Downloaded January 6, 2019)
- 40 Kevin Rector and Alison Knezevich, "Social media companies rescind access to Geofeedia, which fed information to police during 2015 unrest," *The Baltimore Sun*, October 11, 2016. <https://www.baltimoresun.com/news/maryland/crime/bs-md-geofeedia-update-20161011-story.html> (Hereinafter Social Media Companies Rescind Access) (Downloaded January 6, 2019)
- 41 Jack Nicas, "Facebook Says Russian Firms 'Scraped' Data, Some for Facial Recognition," *The New York Times*, October 12, 2018.

<https://www.nytimes.com/2018/10/12/technology/facebook-russian-scraping-data.html> (Downloaded January 6, 2019)

- 42 APIs, or application programming interfaces, are a set of program functions on websites and other computer systems that allow or limit access to data in various ways, including allowing or limit ability to run programs that rapidly take huge quantities of data from a website.
- 43 For more information about our recommendations, see Section IV, “Recommendations.”
- 44 Notable examples advocating for this view of privacy as based on limiting government power to stockpile information about its citizens include:  
Orin Kerr, “An Equilibrium-Adjustment Theory of the Fourth Amendment,” *The Harvard Law Review*, December 20, 2011. <https://harvardlawreview.org/2011/12/an-equilibrium-adjustment-theory-of-the-fourth-amendment/>;  
Daniel Solove, “The Digital Person: Technology and Privacy in the Information Age,” *NYU Press*, October 1, 2004. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2899131](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2899131); Kevin Bankston and Ashkan Soltani, “Tiny Constables and the Cost of Surveillance: Making Cents Out of *United States v. Jones*,” *Yale Law Journal*, January 9, 2014. <https://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones> (All downloaded January 6, 2019)
- 45 *United States v. Jones*, 565 U.S. 400 (2012) (Sotomayor, J., concurring) (Internal citations and quotation marks omitted).
- 46 *Carpenter v. United States*, 585 U.S. \_\_\_\_ (2018) (Internal citations and quotation marks omitted)
- 47 *Carpenter v. United States*, 585 U.S. \_\_\_\_ (2018) (Internal citations and quotation marks omitted)
- 48 The Supreme Court in *Carpenter* explicitly affirms this notion, stating, “A person does not surrender all Fourth Amendment protection by venturing into the public sphere.” *Carpenter v. United States*, 585 U.S. \_\_\_\_ (2018)
- 49 *Carpenter v. United States*, 585 U.S. \_\_\_\_ (2018) (Internal citations and quotation marks omitted)
- 50 *Carpenter v. United States*, 585 U.S. \_\_\_\_ (2018) (Internal citations and quotation marks omitted)
- 51 *United States v. Jones*, 565 U.S. 400 (2012) (Sotomayor, J., concurring, quoting *People v. Weaver*, 12 N. Y. 3d 433, 441–442, 909 N. E. 2d 1195, 1199 (2009))
- 52 “Awareness that the Government may be watching chills associational and expressive freedoms. ...especially in light of the Fourth Amendment’s goal to curb arbitrary exercises of police power to and prevent ‘a too permeating police surveillance.’” *United States v. Jones*, 565 U.S. 400 (2012) (Sotomayor, J., concurring) (internal citations omitted); The Supreme Court has also ruled that

government actions that chill engagement in First Amendment protected activities are a violation of the First Amendment. *Dombrowski v. Pfister*, 380 U.S. 479 (1965)

- 53 In the wake of the Snowden revelations regarding mass NSA surveillance, research found “17% [of American adults] changed their privacy settings on social media; 15% use social media less often; 15% have avoided certain apps and 13% have uninstalled apps; 14% say they speak more in person instead of communicating online or on the phone; and 13% have avoided using certain terms in online communications.” Lee Rainie and Mary Madden, “Americans’ Privacy Strategies Post-Snowden,” Pew Research Center, March 16, 2015. <http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/> (Downloaded January 6, 2019)
- 54 Research found that the Muslim Surveillance Program, which the NYPD operated for nearly a decade, 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,” Creating Law Enforcement Accountability & Responsibility Project, Asian American Legal Defense and Education EFund, and Muslim American Civil Liberties Coalition, June 28, 2012, p. 4. <http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf> (Downloaded January 6, 2019)
- 55 Lawrence Hurley, “Supreme Court restricts police on cellphone location data,” *Reuters*, June 22, 2018. <https://www.reuters.com/article/us-usa-court-mobilephone/supreme-court-rules-warrants-required-for-cellphone-location-data-idUSKBN1JI1WT> (Downloaded February 8, 2018)
- 56 For more information, see section II, “Key Factors.”
- 57 For more information, see section II, “Key Factors.”
- 58 For more information, see section II, “Key Factors.”
- 59 *United States v. Jones*, 565 U.S. 400 (2012); *Carpenter v. United States*, 585 U.S. \_\_\_\_ (2018).
- 60 “In the ‘wild,’ photos rarely contain the frontal images that face recognition algorithms prefer. Poor and uneven lighting can confuse algorithms that rely on facial features or skin textures. Algorithms have an especially tough time mixing photos taken in different circumstances, like mug shots and surveillance camera stills.” Perpetual Line-Up Report, p. 47.
- 61 “Accuracy also drops as databases become larger. Larger databases are more likely to contain lookalikes that mislead face recognition algorithms into picking the wrong matches.” Perpetual Line-Up Report, p. 47; Law enforcement officials using facial recognition are often, especially when using facial recognition for

investigative identification, presented with a candidate list of several individuals that the facial recognition system believes are the most likely matches; false positives stem from officials relying on these suggestions when the candidate lists do not include the actual identity of the person under scrutiny.

- 62 For example, in 2018 Amazon responded to claims that its facial recognition system, Rekognition, had unacceptable rates of inaccuracy by changing the recommended confidence threshold used for finding a match from 80 percent to 95 percent to 99 percent, all during a single week. However, reporting revealed that Amazon actually worked with and supported at least one law enforcement agency using its facial recognition systems with confidence thresholds below 95 percent. ACLU Rekognition Comment; Bryan Menegus, "Defense of Amazon's Face Recognition Tool Undermined by Its Only Known Police Client," *Gizmodo*, January 31, 2019. <https://gizmodo.com/defense-of-amazons-face-recognition-tool-undermined-by-1832238149> (Downloaded February 5, 2019)
- 63 Cost of a False Arrest.
- 64 Some systems are set up to return no candidates if there are none above a set threshold; others will return the top candidates regardless of threshold, or permit officers to change the threshold depending on the number of matches returned. According to the Center on Privacy and Technology, "Face recognition is inherently probabilistic: It does not produce binary 'yes' or 'no' answers, but rather identifies more likely or less likely matches. Most police face recognition systems will output either the top few most similar photos or all photos above a certain similarity threshold." Perpetual Line-Up Report, p. 9.
- 65 For example, the New York Police Department acknowledged in 2015 that it had "misidentified" multiple individuals when it used facial recognition as the basis for identifying suspects. Pei-Sze Cheng, "I-Team: Use of Facial Recognition Technology Expands as Some Question Whether Rules Are Keeping Up," *NBC New York*, June 23, 2015. <https://www.nbcnewyork.com/news/local/Facial-Recognition-NYPD-Technology-Video-Camera-Police-Arrest-Surveillance-309359581.html> (Downloaded January 6, 2019)
- 66 South Wales Police, "Facial Recognition." <https://web.archive.org/web/20181206192450/https://www.south-wales.police.uk/en/advice/facial-recognition-technology/> (Downloaded February 8, 2019); Big Brother Watch, *Face Off: The lawless growth of facial recognition in UK policing*, May 2018, pp. 3-6. <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf> (Downloaded January 6, 2019)
- 67 Bundeskriminalamt (Federal Criminal Police Office of Germany), *Face recognition as a search tool: 'Foto-Fahndung,'* February 2007, pp. 5, 25. [https://www.bka.de/SharedDocs/Downloads/EN/Publications/Other/photographBasedSearchesFinalReport.pdf?\\_\\_blob=publicationFile&v=1](https://www.bka.de/SharedDocs/Downloads/EN/Publications/Other/photographBasedSearchesFinalReport.pdf?__blob=publicationFile&v=1) (Downloaded January 6, 2019)
- 68 For more information, see Section III, "Due Process and Procedural Rights."



- 69 Sidney Fussell, "Axon CEO Says Face Recognition Isn't Accurate Enough for Body Cams Yet," *Gizmodo*, August 8, 2018. <https://gizmodo.com/axon-ceo-says-face-recognition-isnt-accurate-enough-for-1828205723> (Downloaded January 6, 2019)
- 70 Jennifer Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology*, The Electronic Frontier Foundation, February 12, 2018, pp. 1, 22. <https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf> (Downloaded January 6, 2019)
- 71 Dom Galeon, "A New AI That Detects 'Deception' May Bring an End to Lying as We Know It," *Futurism*, January, 9, 2018. <https://futurism.com/new-ai-detects-deception-bring-end-lying-know-it> (Downloaded January 6, 2019)
- 72 *Brown v. Board of Education*, 347 U.S. 483 (1954)
- 73 *Griggs v. Duke Power Co.*, 401 U.S. 424 (1971)
- 74 As a recent example of this occurring, the U.S. District Court for Southern New York held in 2013 that New York City's stop-and-frisk program had systemic discriminatory effects, leading to a settlement and reforms. *Floyd, et al. v. City of New York, et al.*, 959 F. Supp. 2d 540 (2013)
- 75 Alvaro Bedoya, "The Color of Surveillance: What an infamous abuse of power teaches us about the modern spy era," *Slate*, January 18, 2016. <https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html>; Adam Goldman and Matt Apuzzo, "With cameras, informants, NYPD eyed mosques," *Associated Press*, February 23, 2012. <https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques> (All downloaded January 6, 2019)
- 76 *Powell v. Alabama*, 287 US 45 (1932); Equal Justice Initiative, *Lynching in America: Confronting the Legacy of Racial Terror* (3rd Edition), 2017. <https://lynchinginamerica.eji.org/drupal/sites/default/files/2017-07/lynching-in-america-3d-edition-spread.pdf> (Downloaded February 7, 2019); John Lewis et al., *March* (slip edition), Georgia: Top Shelf Productions, September 6, 2016.
- 77 The Sentencing Project, "Racial Disparity." <https://www.sentencingproject.org/issues/racial-disparity/> (Downloaded January 6, 2019); German Lopez, "There are huge racial disparities in how US police use force," *Vox*, November 14, 2018. <https://www.vox.com/identities/2016/8/13/17938186/police-shootings-killings-racism-racial-disparities> (Downloaded January 6, 2019); *Floyd, et al. v. City of New York, et al.*, 959 F. Supp. 2d 540 (2013), finding that New York City's stop-and-frisk program had systemic discriminatory harms. (Downloaded January 6, 2019)
- 78 Joy Buolamwini "Artificial Intelligence Has a Problem With Gender and Racial Bias. Here's How to Solve It," *Time*, February 7, 2019 <http://time.com/5520558/artificial-intelligence-racial-gender-bias/> (Downloaded February 8, 2019); Ramin Skibba, "Hidden algorithms could already be helping compute your fate," *Fast Company*, October 12, 2018. <https://www.fastcompany.com/90249511/hidden-algorithms-could-already-be-helping-compute-your-fate>; Laura Hudson, "Technology Is Biased Too. How

- Do We Fix It?" *FiveThirtyEight*, July 20, 2017. <https://fivethirtyeight.com/features/technology-is-biased-too-how-do-we-fix-it/> (Hereinafter Technology Is Biased Too. How Do We Fix It?) (Downloaded January 6, 2019)
- 79 Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research*, Vol. 81, February 2018. <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>; Steve Lohr, "Facial Recognition Is Accurate, if You're a White Guy," *The New York Times*, February 9, 2018. <https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html> (All downloaded January 6, 2019)
- 80 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> (Downloaded January 6, 2019)
- 81 Brendan Klare et al., "Face Recognition Performance: Role of Demographic Information," *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 6, December 2012, pp. 1789-1801. [http://biometrics.cse.msu.edu/Publications/Face/Klareetal\\_FaceRecognitionPerformance\\_RoleOfDemographicInformation\\_TIFS12.pdf](http://biometrics.cse.msu.edu/Publications/Face/Klareetal_FaceRecognitionPerformance_RoleOfDemographicInformation_TIFS12.pdf) (Downloaded February 7, 2019); Sometimes, such as in the Klare study, higher rates of inaccuracy will be seen in terms of higher rates of false negatives—i.e. being unable to properly identify a match—for people of color and women. This raises serious concerns that law enforcement may engage in improper action because, with systems that return a candidate list, officers will more often be selecting from a list of incorrect suggestions when the subject is a person of color or a woman.
- 82 "The software compares the algorithm against others in the database. It is oblivious to things like a person's hairstyle, gender, race or age." Kameel Stanley, "Face recognition technology proving effective for Pinellas deputies," *Tampa Bay Times*, July 17, 2009. <https://web.archive.org/web/20171014000108/http://www.tampabay.com/news/publicsafety/crime/facial-recognition-technology-proving-effective-for-pinellas-deputies/1019492> (Downloaded February 28, 2019); "An FAQ for the [Seattle Police Department's facial recognition] system says that it 'does not see race, sex, orientation or age.'" *Perpetual Line-Up*, pp. 149.
- 83 Technology Is Biased Too. How Do We Fix It?
- 84 Ava Kofman, "Study: Face Recognition Systems Threaten the Privacy of Millions," *The Intercept*, October 18, 2016. <https://theintercept.com/2016/10/18/study-lack-of-face-recognition-oversight-threatens-privacy-of-millions/> (Downloaded January 6, 2019)
- 85 Rachel Levinson-Waldman, "Why the Surveillance State Is Everybody's Problem," *The Brennan Center for Justice*, May 12, 2015. <https://www.brennancenter.org/blog/why-surveillance-state-everybodys-problem> (Downloaded January 6, 2019)

- 86 National Association for the Advancement of Colored People, "Criminal Justice Factsheet." <https://www.naacp.org/criminal-justice-fact-sheet/> (Downloaded January 6, 2019)
- 87 The Constitution Project, Guidelines for the Use of Body-Worn Cameras by Law Enforcement, December 2016. <https://constitutionproject.org/wp-content/uploads/2016/12/BodyCamerasRptOnline.pdf> (Hereinafter Constitution Project Body-Worn Camera Guidelines) (Downloaded January 6, 2019)
- 88 Sean Rossman, "U.S. drops charges against 129 inauguration day protesters," *USA Today*, January 18, 2018, updated January 19, 2018. <https://www.usatoday.com/story/news/nation-now/2018/01/18/drops-charges-against-129-inauguration-day-protesters-trump/1046324001/> (Downloaded January 6, 2019)
- 89 "As an instrument of surveillance, identification increases the government's power to control individuals' behavior....Anonymity is an important right in a free society in so far as it protects people from bias based on their identities and enables people to vote, speak, and associate more freely by protecting them from the danger of reprisal." International Justice and Public Safety Network, *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field*, June 30, 2011, p. 18. [https://www.eff.org/files/2013/11/07/09 - facial\\_recognition\\_pia\\_report\\_final\\_v2\\_2.pdf](https://www.eff.org/files/2013/11/07/09 - facial_recognition_pia_report_final_v2_2.pdf) (Downloaded January 6, 2019)
- 90 *National Association for the Advancement of Colored People v. Alabama*, 357 U.S. 449 (1958)
- 91 Bench warrants can be for incredibly minor offenses, and apply to huge portions of a community. For example, a 2015 Department of Justice investigation revealed that Ferguson, Missouri, had active, outstanding municipal arrest warrants—mostly for minor offenses such as unpaid fines for traffic violations—for 16,000 people in a municipality with a population of 21,000. Department of Justice Civil Rights Division, *Investigation of the Ferguson Police Department*, March 4, 2015, pp. 3-6, 55. [https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/ferguson\\_police\\_department\\_report\\_1.pdf](https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/ferguson_police_department_report_1.pdf). Social Media Companies Rescind Access.
- 92 Social Media Companies Rescind Access
- 93 Richard W. Vorder Bruegge, "Facial Recognition and Identification Initiatives," Federal Bureau of Investigation, slide 4. [https://www.eff.org/files/filenode/vorder\\_bruegge-facial-recognition-and-identification-initiatives\\_0.pdf](https://www.eff.org/files/filenode/vorder_bruegge-facial-recognition-and-identification-initiatives_0.pdf) (Downloaded January 6, 2019)
- 94 "Rather than attempt to run face matches and identify participants, government could simply develop face prints based on participation, such as 'Baltimore Black Lives Matter Protester #347' or 'Manhattan Mosque Attendee #455.'" Jake Laperruque, "Preserving the Right to Obscurity in the Age of Facial Recognition," The Century Foundation, October 20, 2017. <https://tcf.org/content/report/>

- [preserving-right-obscurity-age-facial-recognition/](#) (Downloaded January 6, 2019)
- 95 Adam Goldman and Matt Apuzzo, "With cameras, informants, NYPD eyed mosques," *Associated Press*, February 23, 2012. <https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques> (All downloaded January 6, 2019)
- 96 42 U.S.C. § 2000aa; U.S. Congress, "Privacy Protection Act of 1980" (P.L. 96-440), Introduced September 21, 1979, by Senator Birch Bayh. <https://www.congress.gov/bill/96th-congress/senate-bill/1790>
- 97 Reporters Committee for Freedom of the Press, "Number of states with shield law climbs to 40," *The News Media and the Law*, Vol. 35, No. 3, Summer 2011, p. 27. <https://www.rcfp.org/journals/news-media-and-law-summer-2011/number-states-shield-law-cl/> (Downloaded January 6, 2019)
- 98 Project On Government Oversight, Government Accountability Project, and Public Employees for Environmental Responsibility, *The Art of Anonymous Activism: Serving the Public While Surviving Public Service*, 2002. [http://www.pogoarchives.org/ebooks/the\\_art\\_of\\_anonymous\\_activism.pdf](http://www.pogoarchives.org/ebooks/the_art_of_anonymous_activism.pdf) (Downloaded January 6, 2019)
- 99 Perpetual Line-Up Report, p. 9.
- 100 *Carpenter v. United States*, 585 U.S. \_\_\_\_ (2018); Stephen Vladeck, "The Supreme Court Phone Location Case Will Decide the Future of Privacy," *Motherboard*, June 16, 2017. [https://motherboard.vice.com/en\\_us/article/59zq5x/scotus-cell-location-privacy-op-ed](https://motherboard.vice.com/en_us/article/59zq5x/scotus-cell-location-privacy-op-ed) (Downloaded January 6, 2019)
- 101 Derivative evidence is evidence that stems from another source, such as materials or documents collected during a police search of a location that was identified by a phone call indicating that the location would contain evidence relevant to the investigation
- 102 Broad use of stingray surveillance was infamously hidden from the public, and even from defendants this surveillance tool was used against, for years. Sam Adler-Bell, "What's Behind the FBI's Obsessive 'Stringray' Secrecy?" The Century Foundation, April 9, 2015. <https://tcf.org/content/commentary/whats-behind-the-fbis-obsessive-stingray-secrecy/> (Hereinafter What's Behind Stingray Secrecy); "Through the use of extensive nondisclosure agreements, the federal government prevents state and local law enforcement from disclosing even the most elementary details of stingray capability and use. Adam Bates, "Stingray: A New Frontier in Police Surveillance," The Cato Institute, January 25, 2017. <https://www.cato.org/publications/policy-analysis/stingray-new-frontier-police-surveillance#full> (All downloaded January 6, 2019)
- 103 Human Rights Watch, *Dark Side: Secret Origins of Evidence in US Criminal Cases*, January 2018, pp. 1-3. <https://www.hrw.org/report/2018/01/09/dark-side-secret-origins-evidence-us-criminal-cases> (Downloaded February 6, 2018)
- 104 Both *Brady v. Maryland*, 373 U.S. 83 (1963) and *Giglio v. United States*, 405 U.S. 150 (1972) require turning over possibly exculpatory

material and prohibit the destruction of such material.

- 105 Perpetual Line-Up Report, pp. 2-3.
- 106 “[Washington County, Oregon] later cited this NDA to justify withholding documents in response to the ACLU’s public records request [for details on its use of facial recognition].” ACLU Rekognition Blog Post; “Amazon marketed its facial recognition tools to Orlando’s police department, providing tens of thousands of dollars of technology to the city at no cost, and shielding the Rekognition pilot with a mutual nondisclosure agreement that kept its details out of the public eye.” Orlando Use of Facial Recognition; Amazon emails included in responses an ACLU records request show county officials discussing “getting an NDA [in order] to get the insight into the Rekognition roadmap.” American Civil Liberties Union Foundation of Florida, “Public Records request related to the Amazon Rekognition facial recognition service,” January 18, 2018, p. 82. [https://www.aclunc.org/docs/20180522\\_ARD.pdf#page=82](https://www.aclunc.org/docs/20180522_ARD.pdf#page=82) (Downloaded January 6, 2019)
- 107 Cell-site simulators imitate cell phone towers to secretly collect the location data of all phones in a given area. American Civil Liberties Union, “Stingray Tracking Devices.” <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices> (Downloaded February 6, 2019); “Through the use of extensive nondisclosure agreements, the federal government prevents state and local law enforcement from disclosing even the most elementary details of stingray capability and use.” What’s Behind Stingray Secrecy.
- 108 Brady rights refers to the requirement established in *Brady v. Maryland* that the government must turn over possibly exculpatory material and prohibit the destruction of such material.
- 109 *United States v. Jones*, 565 U.S. 400 (2012)
- 110 While this report focuses on facial recognition surveillance by government entities, and its recommendations are centered on limiting or requiring certain government actions in relation to facial recognition surveillance, it should be noted that private entities can provide significant aid in enhancing transparency regarding facial recognition surveillance. Most importantly, vendors that provide government entities with facial recognition software or services could disclose all government entities they contract with, and allow an independent entity such as NIST to test the accuracy of their systems and publish the results. Additionally, online services that provide platforms for personal photo and video footage could update transparency reports to indicate whether they receive any government orders requiring facial recognition scans of their photo or video content. Finally, consumer products that incorporate cameras could similarly indicate in transparency reports whether they receive any government orders requiring cameras to be co-opted for real-time facial recognition scans.
- 111 For more information, see section III, “Facial Recognition

Could Damage Evidence and Defendants' Rights"

- 112 We also recommend that facial recognition surveillance be limited to a set of serious crimes. See Recommendation 4.
- 113 We also recommend that facial recognition surveillance be limited to a set of serious crimes. See Recommendation 4.
- 114 We also recommend that facial recognition surveillance be limited to a set of serious crimes. See Recommendation 4.
- 115 Such a system will only be effective if laws also require a minimum confidence threshold for designating matches, which we include in Recommendation 7. Absent such a requirement, the government could simply set extremely low thresholds for "matches," and use those as the basis for police action such as Terry stops (stop-and-frisk), searches, or arrests.
- 116 Constitution Project Body-Worn Camera Guidelines.