GEORGETOWN LAW
Center on Privacy & Technology

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

Before the

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

Hearing on

Law Enforcement's Use of Facial Recognition Technology

Wednesday, March 22, 2017

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

I. Executive Summary

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

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

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

A few key takeaways are below.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

III. How does the FBI use face recognition?

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

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

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

---

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

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

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

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

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

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

III. Problems and Recommendations.

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

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

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

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

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

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

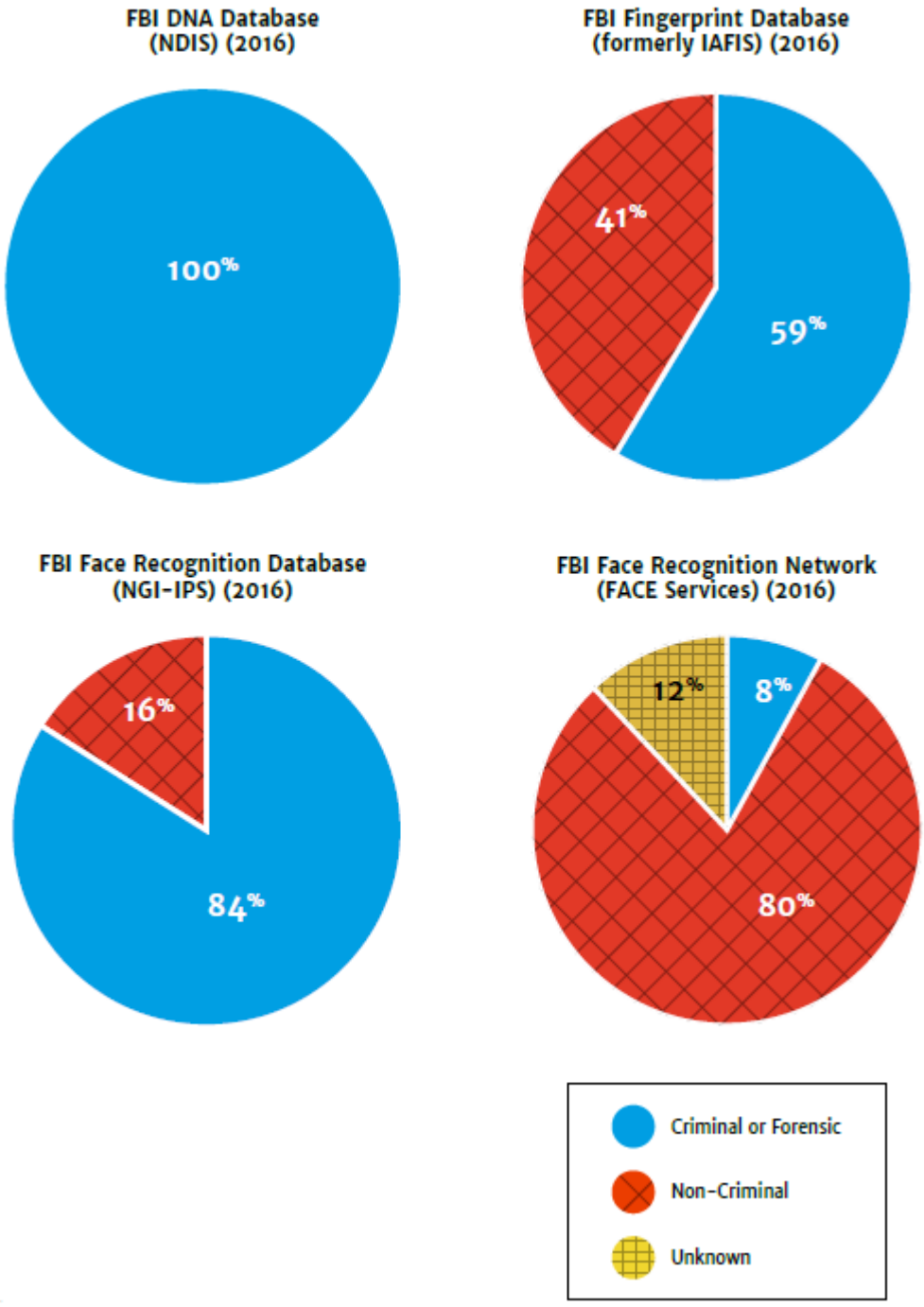
---

[6] Recently, FACE Services has also been able to request searches of U.S. citizen passport photos through a pilot program. *See* GAO-16-267 at 7, n. b.

[7] *The Perpetual Line-Up,* at 25.

[8] *See* note 1 for information on where to find a list of these states.

[9] *See* Federal Highway Administration, *U.S. Department of Transportation, Highway Statistics* (Sept. 2015), *available at* http:// www.fhwa.dot.gov/policyinformation/statistics/2014/pdf/ dl22.pdf*; see* U.S. Census Bureau, *Annual Estimates of the Resident Population for Selected Age Groups by Sex for the*



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

---

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

4. Recommendations.

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

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

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

---

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

[16] 18 U.S.C.A. § 2516.

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

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

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

B. Face recognition may threaten free speech.

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

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

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

---

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

2. Recommendations.

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

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

Agencies would do well to adopt this prohibition.

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

2. Recommendations.

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

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

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

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

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

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

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

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

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

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

2. Recommendations.

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

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

E. Face recognition systems are shrouded in secrecy.

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

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

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

[33] *The Perpetual Line-Up*, at 90 n. 261.
[34] GAO-16-267, at 25.
[35] *See What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing before the Subcomm. on Privacy, Technology & the Law of the S. Comm. on the Judiciary*, 112th Cong., 10–11 (2012) ("One of the things that the MOUs that we sign with the agencies that are going to access the system require is an audit process, so the local agencies are required to audit the use of the system on an annual basis to detect any type of misuse. And then, in addition to that, within our FBI CJIS Division we have an audit unit that goes out and does triennial audits of the same agencies ... a double-check on the audits, as well as to be sure that the audit processes are in place and being done effectively.").

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

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

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

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

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

---

[36] M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003); 5 U.S.C. § 552a(e)(4) (requiring agencies to publish any "establishment or revision of" a system of records in the Federal Register).
[37] *See* Center on Privacy & Technology et. al., *Comment on NPRM 81 Fed. Reg. 27288* (July 6, 2016), https://www.regulations.gov/document?D=DOJOPCL-2016-0008-0114.
[38] *See* 5 U.S.C. § 552a; Implementation, 81 Fed. Reg. 27288, 27829 (proposed May 5, 2016) (to be codified at 28 C.F.R. pt. 16); *see also* Center on Privacy & Technology et. al., *Comment on NPRM 81 Fed. Reg. 27288* (July 6, 2016), https://www.regulations.gov/document?D=DOJOPCL-2016-0008-0114 (explaining impact of proposed exemption of FBI's NGI System from key Privacy Act accountability provisions).
[39] *The Perpetual Line-Up*, at 58, 132.
[40] *The Perpetual Line-Up*, at 89-90 n. 251.
[41] *The Perpetual Line-Up*, at 90 n. 256.
[42] *The Perpetual Line-Up*, at 90 n. 252.
[43] *See* Brady v. Maryland, 373 U.S. 83 (1963).

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

2. Recommendations.

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

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

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

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

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

IV. Conclusion

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

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

---

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